Flowwatch

User Guide

www.flowwatch.com

version: 20200610

Contents:

Flowwatch Overview

Installation:

Basically you will need to deploy Flowwatch into your server.

(1) Download your Flowwatch image from Flowwatch.com

(2) Install the Flowwatch and make sure http://[Flowwatch IP] is up.

(3) Browse to http:// [Flowwatch IP] and use the default username /password to login. The default login username and password are both "admin".

Note: It is essential to change the password right after first login to ensure the security of the system. Please refer to the related pages about how to perform password changes to a specific account.

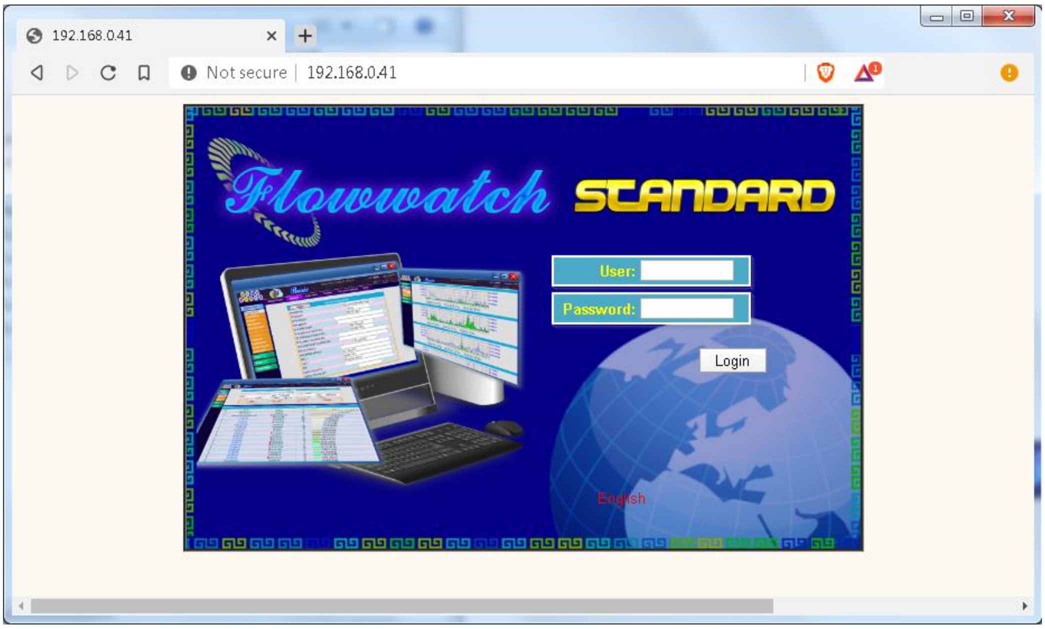


Figure 1 – Web interface Login Page

The follow ports are used for specific purpose, please make sure that there are no other software/service use them.

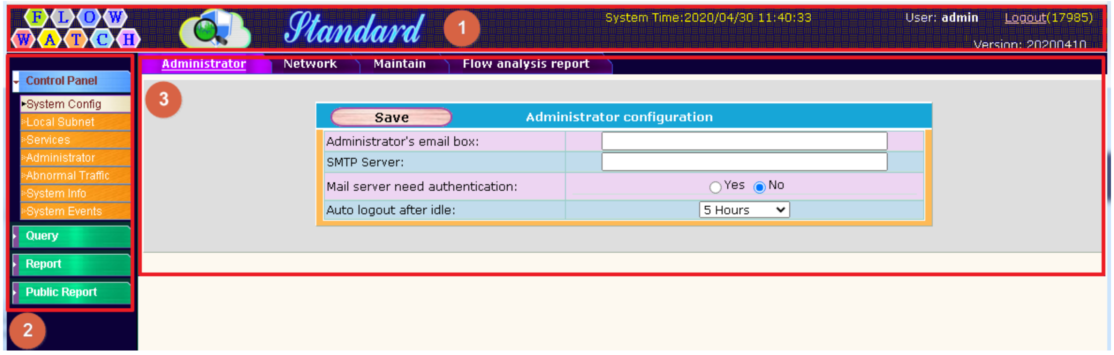
Port Name	Default Port Numbers	Definition
HTTP Port	80	You can connect to Flowwatch from a web browser via 80 port.
Netflow Listener port	9990 / 9991 / 9992	These are the listener port on which Netflow exports are received from routers.

Table 1 – Port Requirements

Web Interface Overview:

Upon successful login, you can see the main page as shown below. The Web interface consists of three parts:

1. The banner area
2. The navigation menu
3. The work area



Administrator's email box:	
SMTP Server:	
Mail server need authentication:	○ Yes ● No
Auto logout after idle:	5 Hours

Figure 2 – Web interface

1. The banner area:

This area has the following parts:

(1) Logo and Model: It shows the Flowwatch logo and the model.

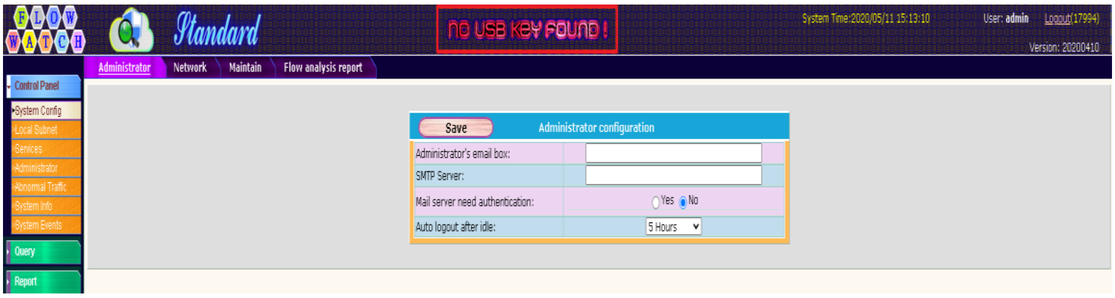
(2) Alerts: If the USB key is not inserted, the alert will be shown here.

(3) Time: The system time will be shown here.

(4) Administration: It shows the login user name here.

(5) Logout: If you want to logout the system, you just need to click the link.

(6) Version: The current version of Flowwatch system.



Administrator's email box:	
SMTP Server:	
Mail server need authentication:	○ Yes ● No
Auto logout after idle:	5 Hours

Figure 3 – Authentication failed

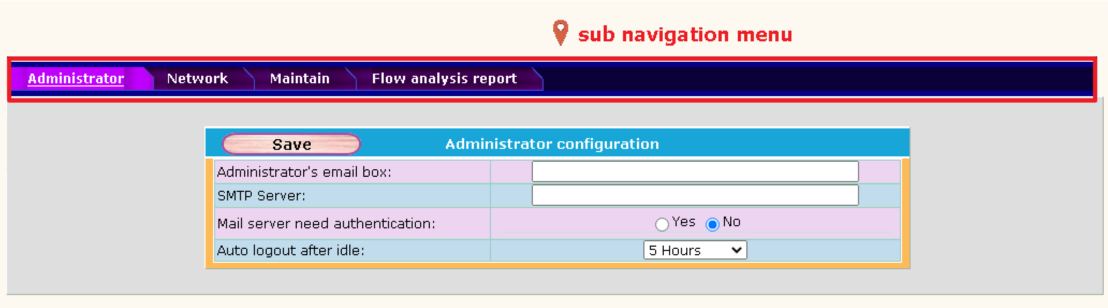
2. The navigation menu:

The navigation menu items can be expanded/collapsed by clicking on them. Below is the list of menu items with the links to their explanations. You can reach the subcategories by clicking the main menu. The primary categories are shown in a different color than the lower-level categories. The main terms and sub-entries will be shown in this area.

(1) Control Panel
(2) Query
(3) Report
(4) Public Report

Note: Not all of the above listed items are visible to the users who are not administrator permission.

3. The work area:
Some navigation menu items may contain lots of configuration page. The sub navigation menu items will be shown in the main work area. You can supply information and make selections that are need to complete the task you selected.



Administrator configuration

Administrator's email box:	
SMTP Server:	
Mail server need authentication:	○ Yes ● No
Auto logout after idle:	5 Hours

Figure 4 – The work area

In the above example, Administrator, Network, Maintain and Flow analysis report are seen as sub navigation menu item.

Icons:
There are some icons appear throughout the web interface.

Icon	Definition
💾	Save
📝	Edit
🗑	Delete

Table 2 – Icon Table

Note: There are some differences between trial version and retail version. We will use the text in blue and italic to display the differences.

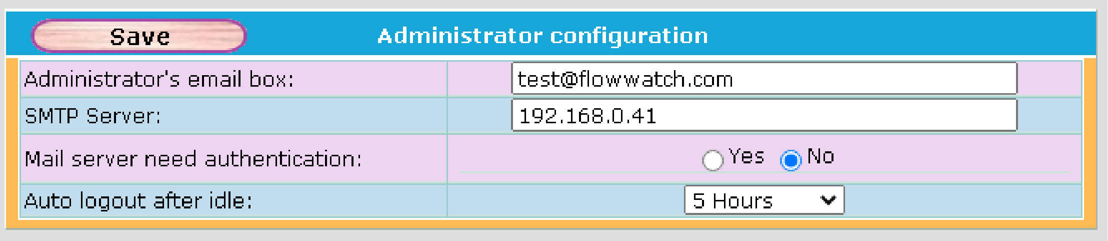
Control Panel

System Config:

Administrator

The administrator can set up the email notifications and change the inactivity timeout value here. The Administrator’s email box is the email address(es) that you want to receive the alerts on.

Note: Separate multiple email addresses with commas. Flowwatch system will fill the first email address into the ‘From(Sent as)’ field of notification.



Administrator's email box:	test@flowwatch.com
SMTP Server:	192.168.0.41
Mail server need authentication:	○ Yes ● No
Auto logout after idle:	5 Hours

Figure 5 – Email notifications setting

Network

The settings in the Network configuration form are:

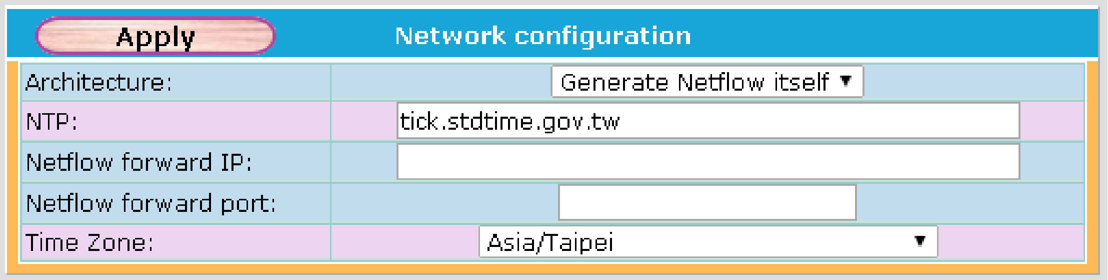
- **Architecture:** You can select **Receive Netflow** or **Generate Netflow itself** as Data source.

Note: When you select **Receive Netflow**, you need to configure switches to send Netflow to Flowwatch. You can use **9990/9991/9992** as the destination port.

- **NTP:** You can specify a IP address of NTP server in this field.

By filling out the following two fields, you can forward the Netflow Data to other device.

- **Netflow forward IP:**
- Netflow forward port:
- **Time Zone:** You can use the **Time Zone** drop-down menu and select the correct zone setting.



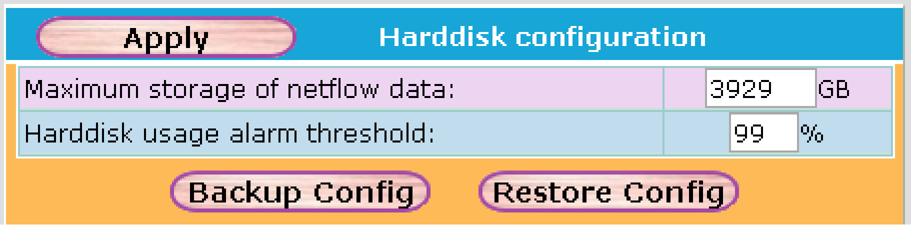
Architecture:	Generate Netflow itself
NTP:	tick.stdtime.gov.tw
Netflow forward IP:	
Netflow forward port:	
Time Zone:	Asia/Taipei

Figure 6 – Network configuration

Maintain

You can enter the capacity that used to store the netflow data. You can also set up the threshold of alarm system. If the disk usage exceeds the threshold, the system will send an email to the administrator. You can create backups of your Flowwatch system's current configuration, and restore it if necessary. It is recommended that you regularly make backups.

Note: The system will send the notification at 4 o'clock (in the morning).



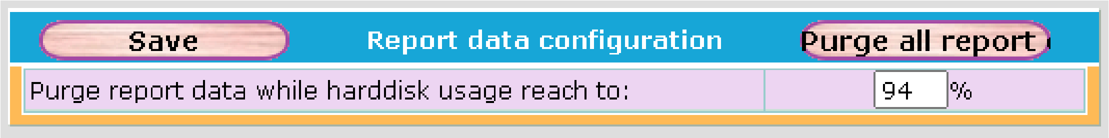
Harddisk configuration

Maximum storage of netflow data:	3929 GB
Harddisk usage alarm threshold:	99 %

Figure 7 – Network configuration

Flow analysis report

By clicking the **Purge all report** button on the top right corner, you can purge all reports and logs in the flowwatch system. You can also change the purge setting.



Report data configuration

Purge report data while harddisk usage reach to:	94 %

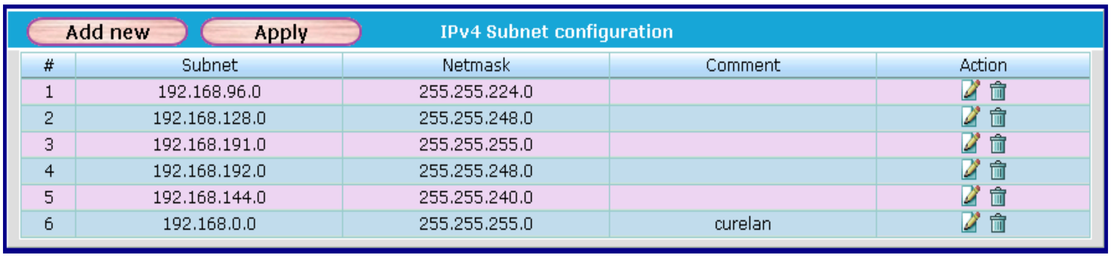
Figure 8 – Report data configuration

Note: The purge report threshold must always be less than the hard disk usage threshold.

Local Subnet:

IPv4 Local Subnet

You need to define the local subnets that you want to monitor. You can add a new one by clicking the **Add new** button on the top left corner and then filling in the information and click the **save** icon. After you add all desired subnets to the Flowwatch, you need to click the **Apply** button so that the setting will be applied.



#	Subnet	Netmask	Comment	Action
1	192.168.96.0	255.255.224.0		✎ 🗑
2	192.168.128.0	255.255.248.0		✎ 🗑
3	192.168.191.0	255.255.255.0		✎ 🗑
4	192.168.192.0	255.255.248.0		✎ 🗑
5	192.168.144.0	255.255.240.0		✎ 🗑
6	192.168.0.0	255.255.255.0	curelan	✎ 🗑

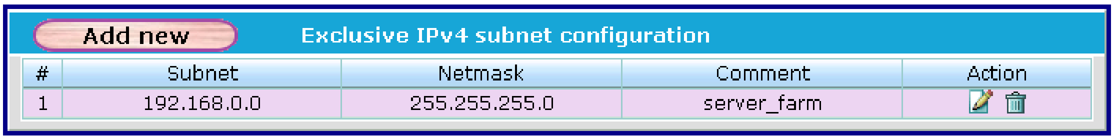
Figure 9 – Local subnet setting

Local subnets exclude from public report

You can filter out the specific IP addresses or subnets from the public report by making the filter. If you have multiple IP addresses or subnets to exclude, you can make multiple filters. You can add a new one by clicking the **Add new** button on the top left corner.

Example:

If you want to filter out a subnet of IP addresses like 192.168.0.*, you can set up the filter like the following figure shown.

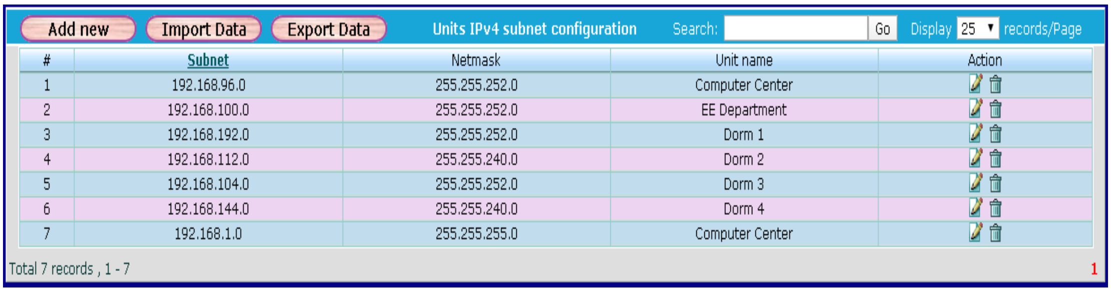


#	Subnet	Netmask	Comment	Action
1	192.168.0.0	255.255.255.0	server_farm	✎ 🗑

Figure 10 – Set the exclude filter for the public report

IPv4 Subnet of each unit

This setting allows you to create groups based on the IP address for reporting purpose in Flowwatch.



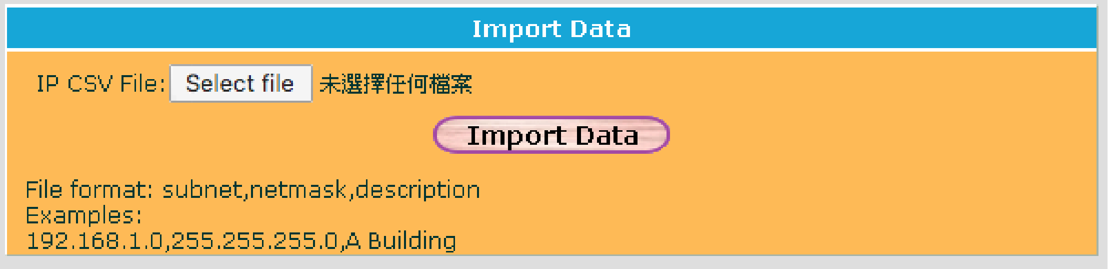
#	Subnet	Netmask	Unit name	Action
1	192.168.96.0	255.255.252.0	Computer Center	✎ 🗑
2	192.168.100.0	255.255.252.0	EE Department	✎ 🗑
3	192.168.192.0	255.255.252.0	Dorm 1	✎ 🗑
4	192.168.112.0	255.255.240.0	Dorm 2	✎ 🗑
5	192.168.104.0	255.255.252.0	Dorm 3	✎ 🗑
6	192.168.144.0	255.255.240.0	Dorm 4	✎ 🗑
7	192.168.1.0	255.255.255.0	Computer Center	✎ 🗑

Total 7 records , 1 - 7 1

Figure 11 – Unit's subnet configuration

You can create a new group by clicking the **Add new** button. All you have to do is filling in the information and click the **save** icon. The system allows you to export the data by clicking **Export Data** button. The data will be saved as a CSV file on your client computer. A file select dialog box pops up, you have to enter or select a file name and click 'save' in order to have the file actually stored. You can also import your data to the system by clicking the **Import Data** button. You need to select the file that you want to import and then click the **Import Data** button.

Note: The Flowwatch system can only read a CSV file in fixed format.



Import Data

IP CSV File: Select file 未選擇任何檔案

Import Data

File format: subnet,netmask,description
Examples:
192.168.1.0,255.255.255.0,A Building

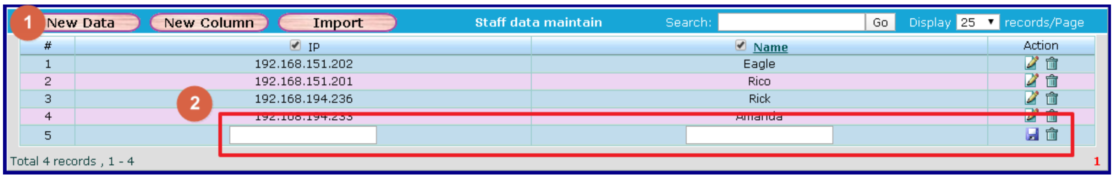
Figure 12 – Import Data to the unit's subnet configuration

People Data

You can create a relationship between IP address and its user. Sometimes you may want to make the report content more readable. The system allows you can create a relationship between IP address and its user. You can also add a custom column into the report.

Follow the steps to create a new mapping relationship:

#	Description
Step 1	Click the **New Data** button on the top left corner.
Step 2	Fill data into the form and then click the **save** icon.



#	☑ IP	☑ Name	Action
1	192.168.151.202	Eagle	
2	192.168.151.201	Rico	
3	192.168.194.236	Rick	
4	192.168.194.233	Amanda	
5			

Total 4 records , 1 - 4 1

Figure 13 – Add a new data in the staff data table

Follow the steps to create a new column:

#	Description
Step 1	Click the **New Column** button
Step 2	Specify the name of the new column and then click the **save** icon.

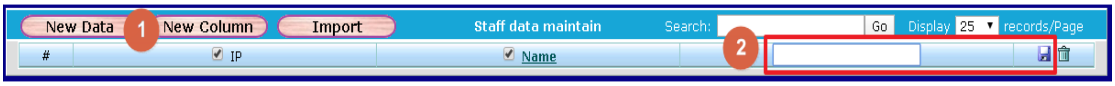


Figure 14 – Add a custom column into the report

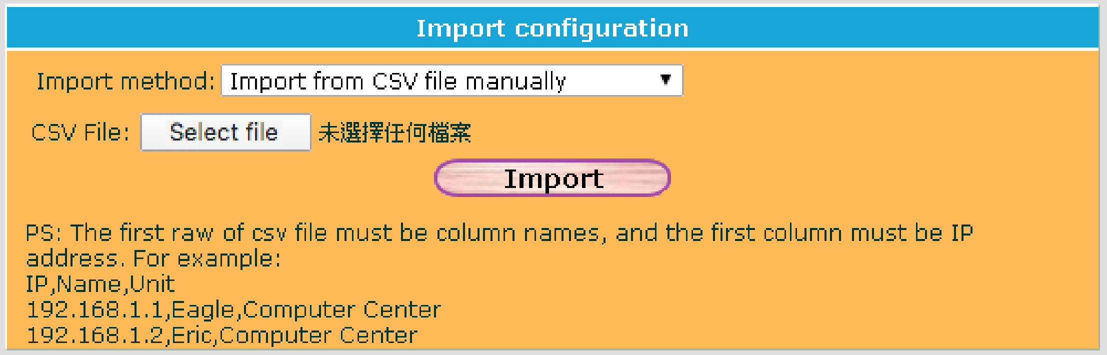
There are two ways that you can choose to import the data.

1. Import the CSV file manually:

(1) Select **Import from CSV file manually**.

(2) You need to click the **Select file** button and then select the file that you want to import.

(3) Click the **Import** button, the import file will be imported.



Import configuration

Import method: Import from CSV file manually

CSV File: Select file 未選擇任何檔案

Import

PS: The first raw of csv file must be column names, and the first column must be IP address. For example:
IP,Name,Unit
192.168.1.1,Eagle,Computer Center
192.168.1.2,Eric,Computer Center

Figure 15 – Manually import a file into the system

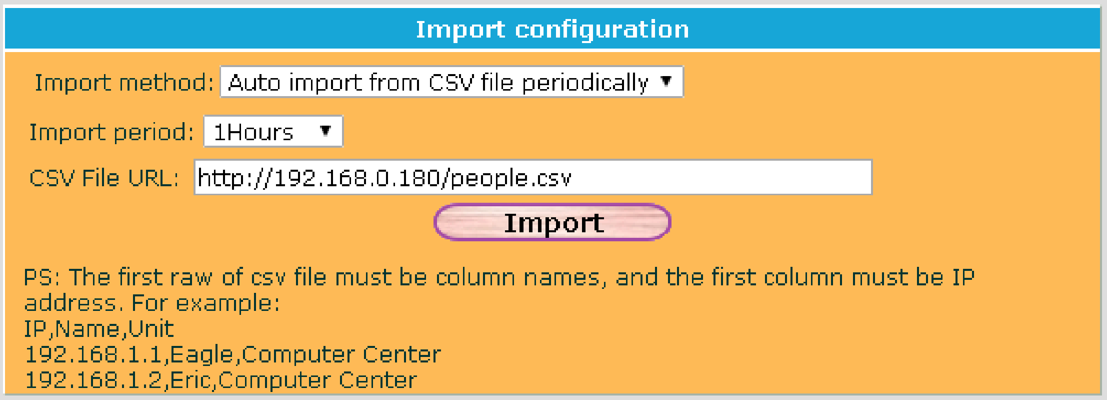
2. Automatically import data into Flowwatch:

(1) Select **Auto import from CSV file periodically**.

(2) Select the time interval for file updating.

(3) Enter the file path location.

(4) Click on the **Import** button to save the setting.



Import configuration

Import method: Auto import from CSV file periodically

Import period: 1Hours

CSV File URL: http://192.168.0.180/people.csv

Import

PS: The first raw of csv file must be column names, and the first column must be IP address. For example:
IP,Name,Unit
192.168.1.1,Eagle,Computer Center
192.168.1.2,Eric,Computer Center

Figure 16 – Import a file into the system automatically

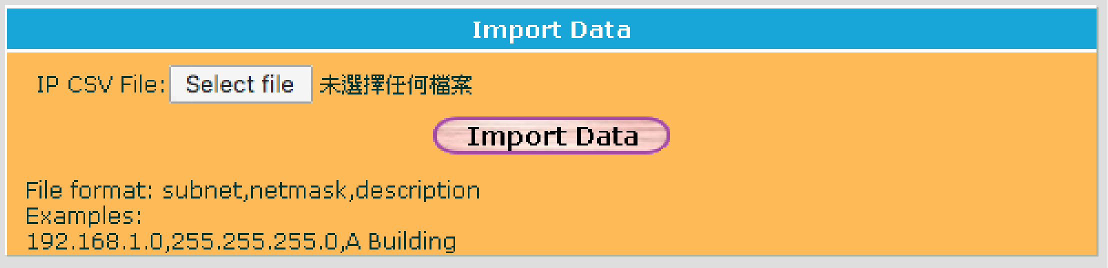
Note: If the checkbox in column header is checked, the header and data will be displayed in the report.

Note: The Flowwatch can only read a CSV file in fixed format.

IPv4 subnet of outside units

This setting allows you to create groups for outsider units based on the IP address for reporting purpose in Flowwatch. You can create a new group by clicking the **Add new** button. All you have to do is filling in the information and click the **save** icon. The system allows you to export the data by clicking **Export Data** button. The data will be saved as a CSV file on your client computer. A file select dialog box pops up, you have to enter or select a file name and click 'save' in order to have the file actually stored. You can also import your data to the system by clicking the **Import Data** button. You need to select the file that you want to import and then click the **Import Data** button.

Note: The Flowwatch system can only read a CSV file in fixed format.



Import Data

IP CSV File: Select file 未選擇任何檔案

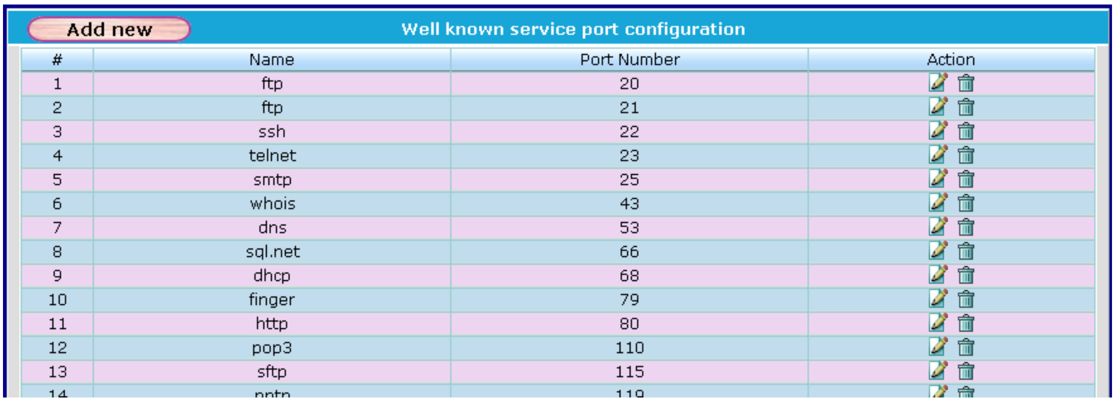
Import Data

File format: subnet,netmask,description
Examples:
192.168.1.0,255.255.255.0,A Building

Figure 17 – Import Data to the outsider unit

Services:

Port numbers range are from 0 to 65535, but the first 1024 ports are reserved for privileged services and designated as well-known ports. You can add/edit/delete an entry by yourself. It can be applied to the filter: protocol to a report.



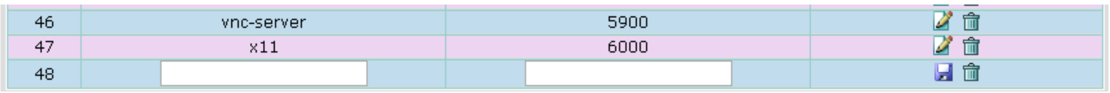
Add new — Well known service port configuration

#	Name	Port Number	Action
1	ftp	20	✎ 🗑
2	ftp	21	✎ 🗑
3	ssh	22	✎ 🗑
4	telnet	23	✎ 🗑
5	smtp	25	✎ 🗑
6	whois	43	✎ 🗑
7	dns	53	✎ 🗑
8	sql.net	66	✎ 🗑
9	dhcp	68	✎ 🗑
10	finger	79	✎ 🗑
11	http	80	✎ 🗑
12	pop3	110	✎ 🗑
13	sftp	115	✎ 🗑
14	nntp	119	✎ 🗑

Figure 18 – Some of the well-known ports

To add a new entry, click the **Add new** button. You can fill out the fields and then click **Save** icon.

Note: One service name can have many port numbers. One port number can only be in one service name. It is a one-to-many relationship.



46	vnc-server	5900	✎ 🗑
47	x11	6000	✎ 🗑
48			💾 🗑

Figure 19 – Add new port service

Administrator:

User management

1. To add a user to the system, click the **Add new** button.

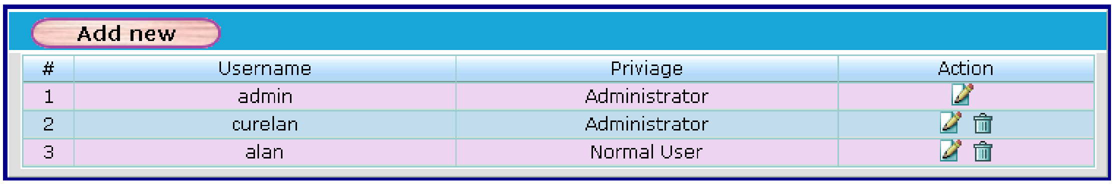
You can specify the username, password and privilege in the page. If the user to be added will have administrator privileges, select Administrator in the drop-down list. There are two principal access levels:

(a) Administrator: Read-write access. The administrator credentials allow changes to be made to all system parameters.

(b) Normal user: Read-only access. The normal user credentials permit viewing reports but prevent making and saving changes.

2. To update the user information, click the **Edit** icon and then change the fields as desired. After you finish your change, click the **Save** button.

3. To delete the user from system, click **Delete** icon.

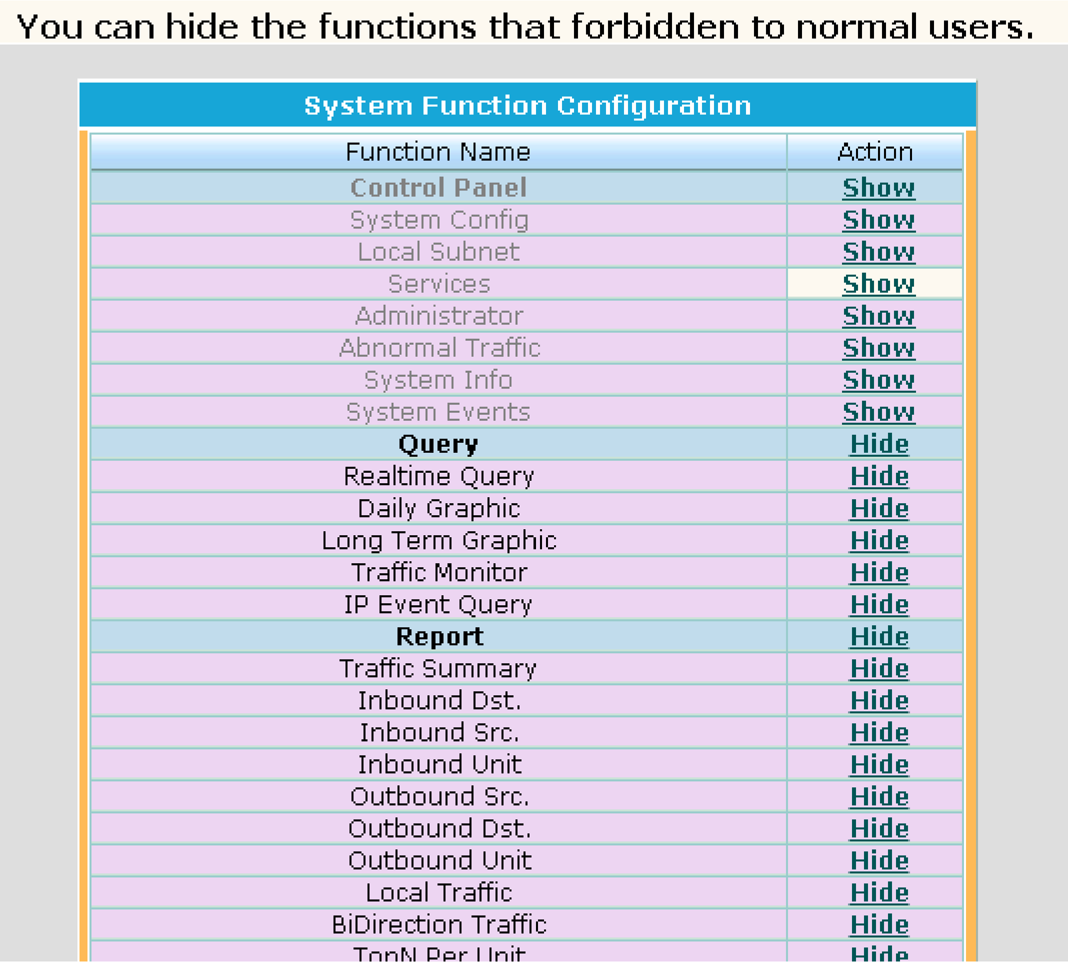


#	Username	Priviage	Action
1	admin	Administrator	✎
2	curelan	Administrator	✎ 🗑
3	alan	Normal User	✎ 🗑

Figure 20 –The interface of User management

Function management

In this page, you can set which functions that can be shown to normal user.



You can hide the functions that forbidden to normal users.

System Function Configuration

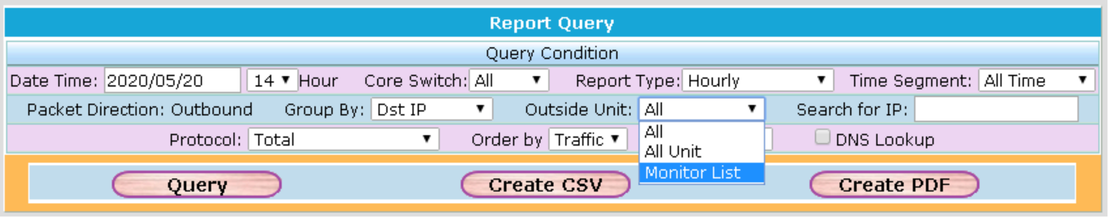
Function Name	Action
Control Panel	Show
System Config	Show
Local Subnet	Show
Services	Show
Administrator	Show
Abnormal Traffic	Show
System Info	Show
System Events	Show
Query	Hide
Realtime Query	Hide
Daily Graphic	Hide
Long Term Graphic	Hide
Traffic Monitor	Hide
IP Event Query	Hide
Report	Hide
Traffic Summary	Hide
Inbound Dst.	Hide
Inbound Src.	Hide
Inbound Unit	Hide
Outbound Src.	Hide
Outbound Dst.	Hide
Outbound Unit	Hide
Local Traffic	Hide
BiDirection Traffic	Hide
TopN Per Unit	Hide

Figure 21 – Function management

Abnormal Traffic:

Abnormal traffic monitor list

Flowwatch allows the administrator to add monitor list as the report filter condition for ‘Inbound Src.’/’Outbound Dst.’ report.



Report Query

Query Condition

Date Time: 2020/05/20 14 Hour Core Switch: All Report Type: Hourly Time Segment: All Time

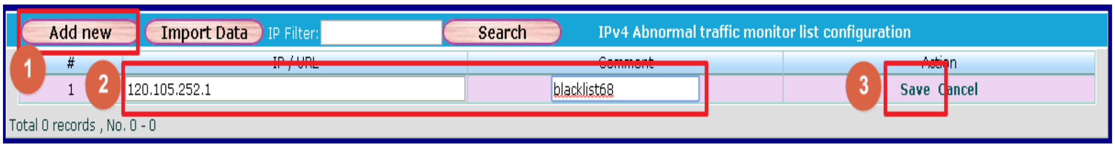
Packet Direction: Outbound Group By: Dst IP Outside Unit: All Search for IP:

Protocol: Total Order by Traffic □ DNS Lookup

Figure 22 – Use monitor list as a filter condition

Follow the steps to create a new monitor list:

#	Description
Step 1	Click the **Add new** button
Step 2	Specify the IP address and Comment
Step 3	Click the '**Save**' to save the setting



#	IP / URL	Comment	Action
1	120.105.252.1	blacklist68	Save Cancel

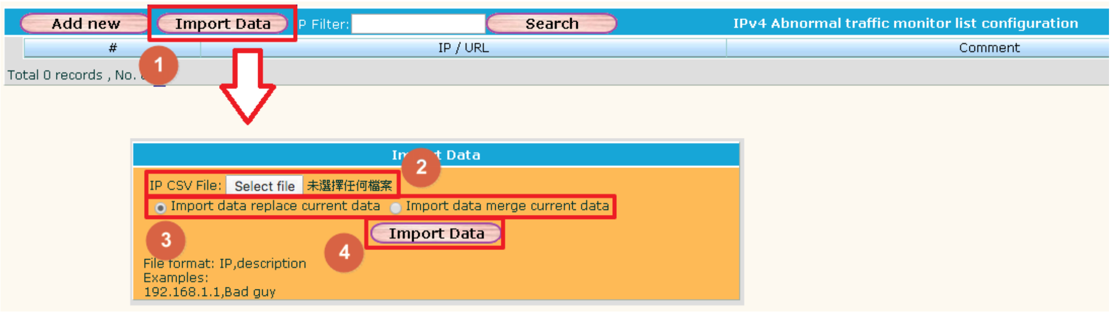
Total 0 records , No. 0 - 0

Figure 23 – Add a new record to the monitor list

Follow the steps to import a CSV file for the monitor list:

#	Description
Step 1	Click the **Import Data** button
Step 2	Click **Select file** button and select the file that you want to import
Step 3	You can choose to overlay or merge with the existing records
Step 4	Click the **Import Data** button

Note: The Flowwatch system can only read a CSV file in fixed format.



Total 0 records , No.

IP CSV File: Select file 未選擇任何檔案

● Import data replace current data ○ Import data merge current data

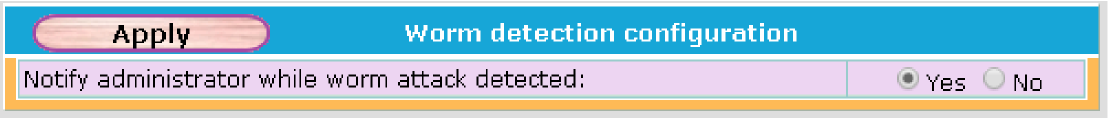
File format: IP,description
Examples:
192.168.1.1,Bad guy

Figure 24 – Import records to the monitor list

The flowwatch allows administrator to configure individual anomalous behavior detection. If you want to receive the email alerts, please make sure the email alerts are tuned on in each of the detection settings page.

Worm Detection

When a worm detection is triggered, the specified email addresses will receive an email with information about what happened.



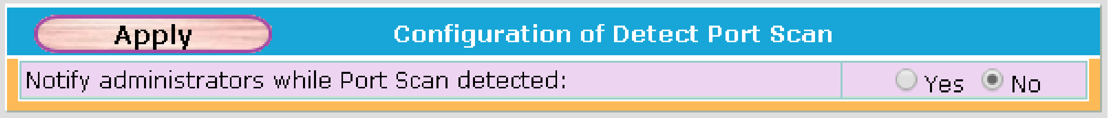
Worm detection configuration

Notify administrator while worm attack detected: ● Yes ○ No

Figure 25 – Worm notification setting

Detect Port Scan

When a port scanning detection is triggered, the specified email addresses will receive an email with information about what happened.



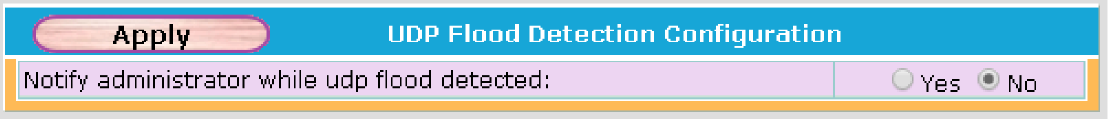
Configuration of Detect Port Scan

Notify administrators while Port Scan detected: ○ Yes ● No

Figure 26 – Port scanning notification setting

UDP Flood Detection

When a UDP flooding detection is triggered, the specified email addresses will receive an email with information about what happened.



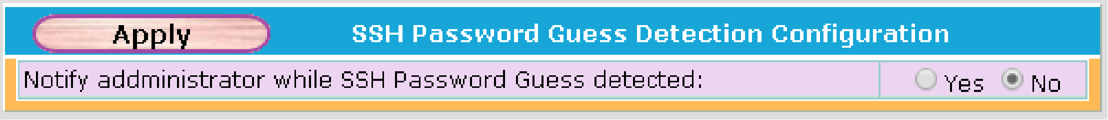
UDP Flood Detection Configuration

Notify administrator while udp flood detected: ○ Yes ● No

Figure 27 – UDP flooding notification setting

SSH Password Guess Detection

When a SSH password guess detection is triggered, the specified email addresses will receive an email with information about what happened.



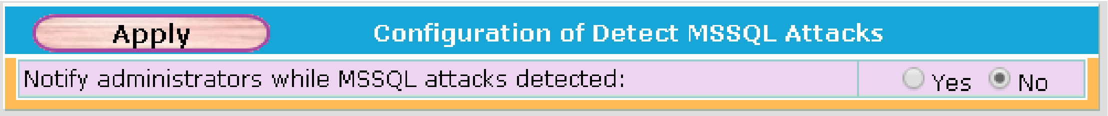
SSH Password Guess Detection Configuration

Notify addministrator while SSH Password Guess detected: ○ Yes ● No

Figure 28 – SSH notification setting

Detect MSSQL Attacks

When a MSSQL attack is detected, the specified email addresses will receive an email with information about what happened.



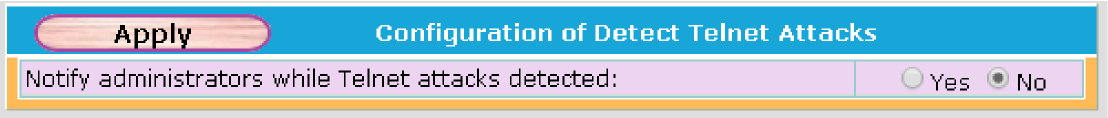
Configuration of Detect MSSQL Attacks

Notify administrators while MSSQL attacks detected: ○ Yes ● No

Figure 29 – MSSQL notification setting

Detect Telnet Attacks

When a telnet attack is detected, the specified email addresses will receive an email with information about what happened.



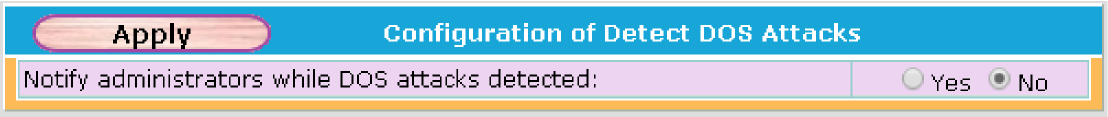
Configuration of Detect Telnet Attacks

Notify administrators while Telnet attacks detected: ○ Yes ● No

Figure 30 – Telnet notification setting

Detect DOS Attacks

When a DOS attack is detected, the specified email addresses will receive an email with information about what happened.



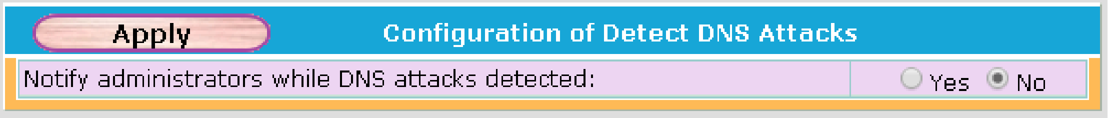
Configuration of Detect DOS Attacks

Notify administrators while DOS attacks detected: ○ Yes ● No

Figure 31 – DOS notification setting

Detect DNS Attacks

When a DNS attack is detected, the specified email addresses will receive an email with information about what happened.



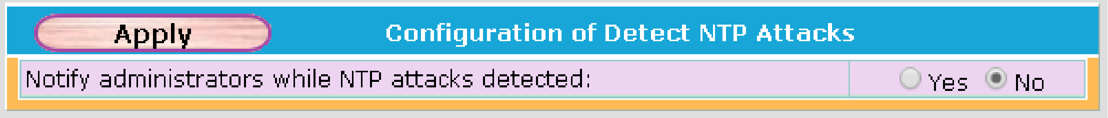
Configuration of Detect DNS Attacks

Notify administrators while DNS attacks detected: ○ Yes ● No

Figure 32 – DNS notification setting

Detect NTP Attacks

When a NTP attack is detected, the specified email addresses will receive an email with information about what happened.



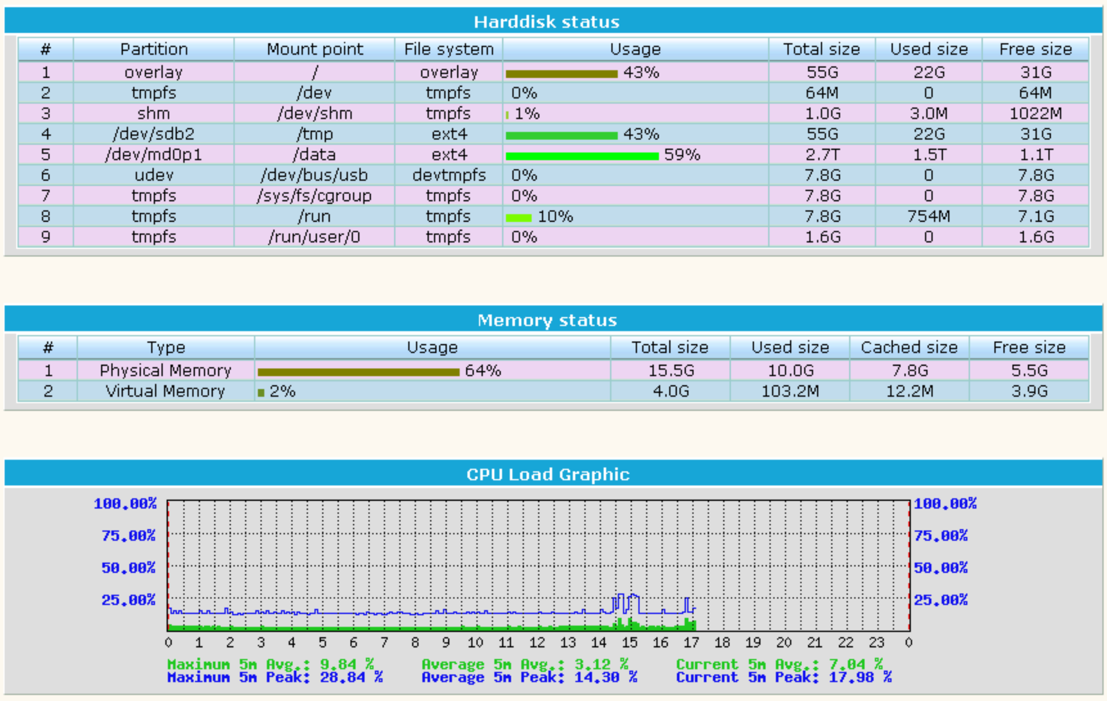
Configuration of Detect NTP Attacks

Notify administrators while NTP attacks detected: ○ Yes ● No

Figure 33 – NTP notification setting

System Info:

This part of page provides the hardware utilization, such as the utilization of CPUs, memory and the hard drive usage.



Harddisk status

#	Partition	Mount point	File system	Usage	Total size	Used size	Free size
1	overlay	/	overlay	43%	55G	22G	31G
2	tmpfs	/dev	tmpfs	0%	64M	0	64M
3	shm	/dev/shm	tmpfs	1%	1.0G	3.0M	1022M
4	/dev/sdb2	/tmp	ext4	43%	55G	22G	31G
5	/dev/md0p1	/data	ext4	59%	2.7T	1.5T	1.1T
6	udev	/dev/bus/usb	devtmpfs	0%	7.8G	0	7.8G
7	tmpfs	/sys/fs/cgroup	tmpfs	0%	7.8G	0	7.8G
8	tmpfs	/run	tmpfs	10%	7.8G	754M	7.1G
9	tmpfs	/run/user/0	tmpfs	0%	1.6G	0	1.6G

Memory status

#	Type	Usage	Total size	Used size	Cached size	Free size
1	Physical Memory	64%	15.5G	10.0G	7.8G	5.5G
2	Virtual Memory	2%	4.0G	103.2M	12.2M	3.9G

CPU Load Graphic

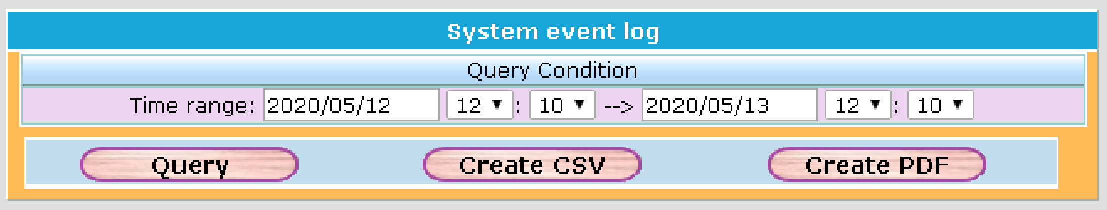
```
Maximum 5m Avg.: 9.84 %     Average 5m Avg.: 3.12 %     Current 5m Avg.: 7.04 %
Maximum 5m Peak: 28.84 %    Average 5m Peak: 14.30 %    Current 5m Peak: 17.98 %
```

Figure 34 – Hardware utilization

Note: By default, a container has no resource constraints and can use as much of a given resource. Therefore, the host might have a 'out of memory' problem when there are multiple containers.

System Events:

To check the event logs, go to the **System Events**. You can define the time range to be displayed in the report. After you specify the range of records to be displayed. Then, click **Query** button. The filtered data will be displayed and sorted by the time when they were originated. The **Create CSV**/**Create PDF** button lets you save the report as a CSV/PDF file on your client computer. A file select dialog box pops up, you have to enter or select a file name and click 'save' in order to have the file actually stored.

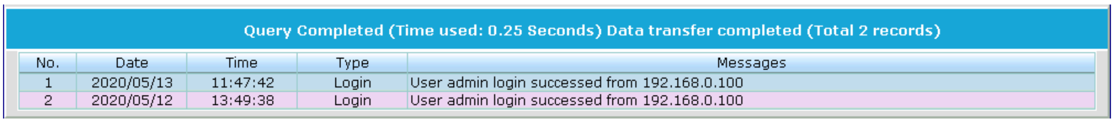


System event log

Query Condition

Time range: 2020/05/12 12 ▼ : 10 ▼ --> 2020/05/13 12 ▼ : 10 ▼

Figure 35 – The System Events window



Query Completed (Time used: 0.25 Seconds) Data transfer completed (Total 2 records)

No.	Date	Time	Type	Messages
1	2020/05/13	11:47:42	Login	User admin login successed from 192.168.0.100
2	2020/05/12	13:49:38	Login	User admin login successed from 192.168.0.100

Figure 36 – The filtered data will be displayed

Query

Real-time Query:

The Flowwatch can provide the dynamic filtering displaying historical traffic results. The administrator can use this feature to identify some malicious traffic. You can export the results of a report to a PDF/CSV file by click the '**Create PDF**'/'**Create CSV** ' button.

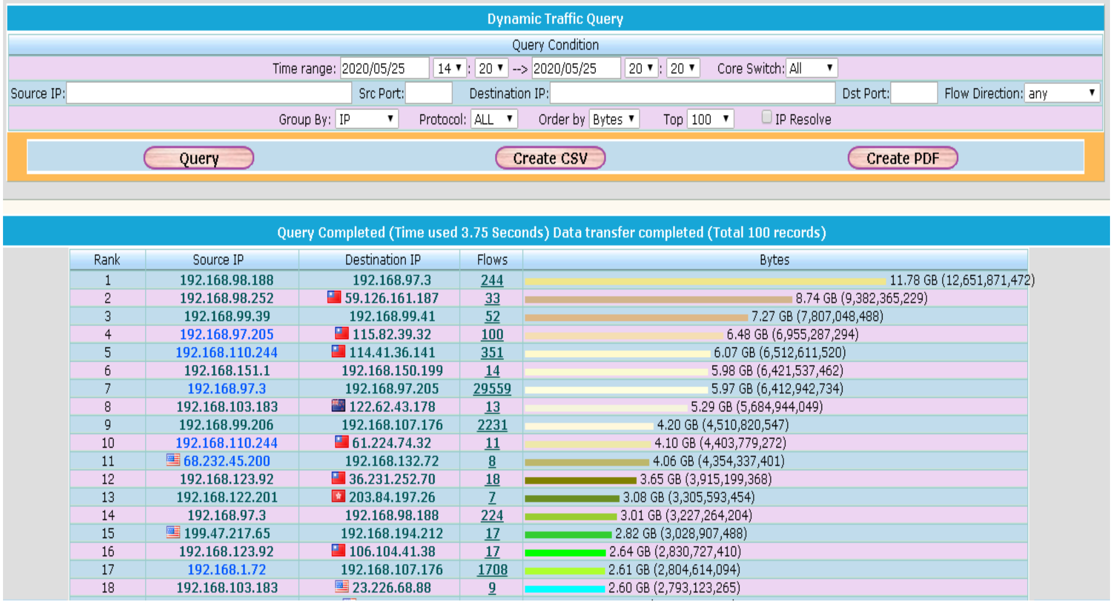
Possible condition types are described below:

- **Time range:** You can specify the time periods for the report.
- **Core Switch:** You can specify the data source for the report.

The relationship between core switch number and listener port number :

Core Switch #	Listener port #
Core 1	9990
Core 2	9991
Core 3	9992
All	9991, 9992 and 9993

- **Source IP:** You can specify an IP address as the source IP.
- **Src Port:** You can specify a port number as the source port number.
- **Destination IP:** You can specify an IP address as the destination IP.
- **Dst Port:** You can specify a port number as the destination port number.
- **Flow Direction:** In which direction should data be accounted? Local, Inbound, Outbound, Bidirectional or any?
- **Group by:** You can group data by IP, Source port number or destination port number.
- **Protocol:** In which protocol should data be accounted? All, TCP, UDP, ICMP or IGMP?
- **Order by:** To sort the result by traffic or flow.
- **Top:** It will list the first N records in this report.



Dynamic Traffic Query

Query Condition

Time range: 2020/05/25 14 : 20 --> 2020/05/25 20 : 20 Core Switch: All

Source IP: Src Port: Destination IP: Dst Port: Flow Direction: any

Group By: IP Protocol: ALL Order by Bytes Top 100 □ IP Resolve

Query Completed (Time used 3.75 Seconds) Data transfer completed (Total 100 records)

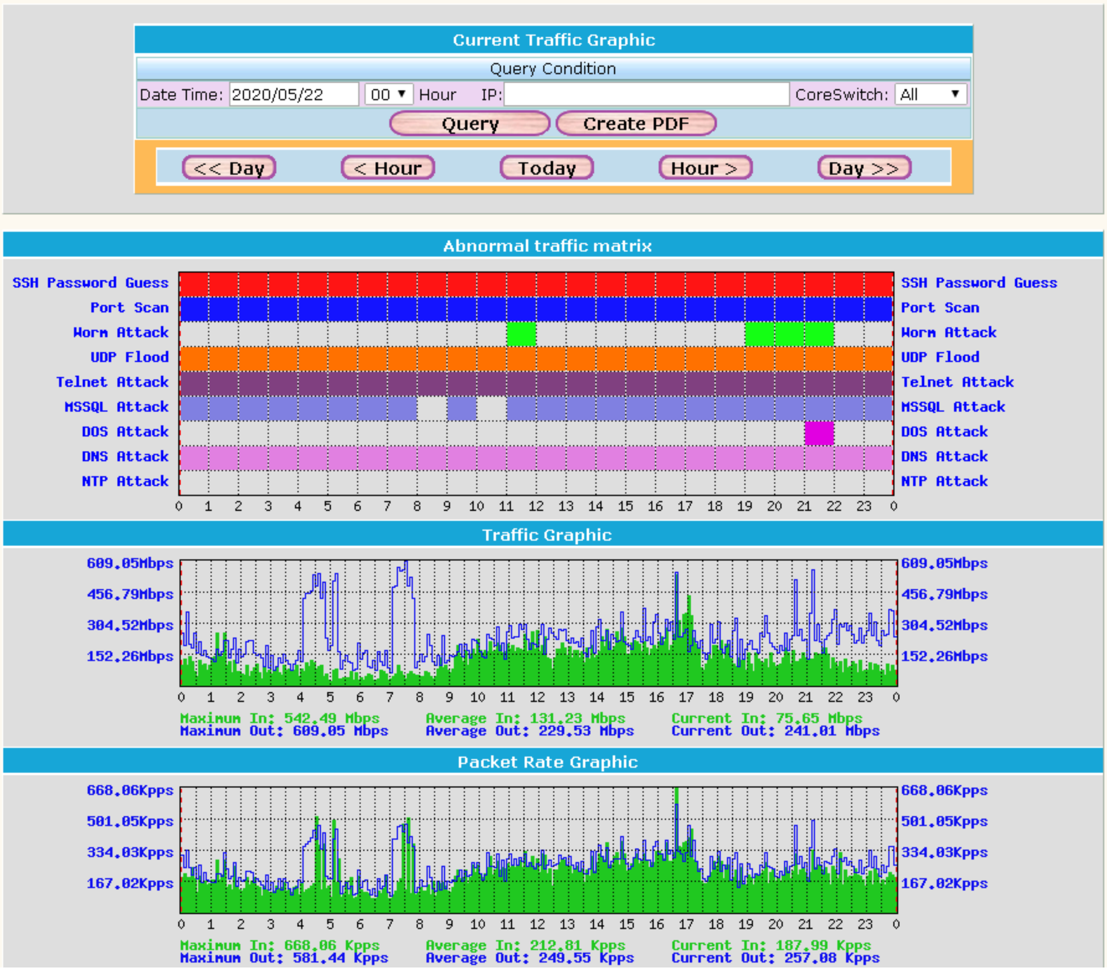
Rank	Source IP	Destination IP	Flows	Bytes
1	192.168.98.188	192.168.97.3	244	11.78 GB (12,651,871,472)
2	192.168.98.252	59.126.161.187	33	8.74 GB (9,382,365,229)
3	192.168.99.39	192.168.99.41	52	7.27 GB (7,807,048,488)
4	192.168.97.205	115.82.39.32	100	6.48 GB (6,955,287,294)
5	192.168.110.244	114.41.36.141	351	6.07 GB (6,512,611,520)
6	192.168.151.1	192.168.150.199	14	5.98 GB (6,421,537,462)
7	192.168.97.3	192.168.97.205	29559	5.97 GB (6,412,942,734)
8	192.168.103.183	122.62.43.178	13	5.29 GB (5,684,944,049)
9	192.168.99.206	192.168.107.176	2231	4.20 GB (4,510,820,547)
10	192.168.110.244	61.224.74.32	11	4.10 GB (4,403,779,272)
11	68.232.45.200	192.168.132.72	8	4.06 GB (4,354,337,401)
12	192.168.123.92	36.231.252.70	18	3.65 GB (3,915,199,368)
13	192.168.122.201	203.84.197.26	7	3.08 GB (3,305,593,454)
14	192.168.97.3	192.168.98.188	224	3.01 GB (3,227,264,204)
15	199.47.217.65	192.168.194.212	17	2.82 GB (3,028,907,488)
16	192.168.123.92	106.104.41.38	17	2.64 GB (2,830,727,410)
17	192.168.1.72	192.168.107.176	1708	2.61 GB (2,804,614,094)
18	192.168.103.183	23.226.68.88	9	2.60 GB (2,793,123,265)

Figure 37 – Dynamic Traffic Query

Note: The trial version can only display the first 10 records.

Daily Graphic:

The Flowwatch can provide the abnormal traffic matrix and the Multi Router Traffic Grapher (MRTG). The abnormal traffic matrix is arranged in a 9-scene-deep-by-24-track-wide grid. It lets you know exactly what had happened in each day. The grid will light up if an event occurred. You can read the report by clicking on the grid. You can export the results of a report to a PDF file by click the **Create PDF** button.



Current Traffic Graphic

Query Condition

Date Time: 2020/05/22 00 Hour IP: CoreSwitch: All

Maximum In: 542.49 Mbps Average In: 131.23 Mbps Current In: 75.65 Mbps
Maximum Out: 609.05 Mbps Average Out: 229.53 Mbps Current Out: 241.01 Mbps

Maximum In: 668.06 Kpps Average In: 212.81 Kpps Current In: 187.99 Kpps
Maximum Out: 581.44 Kpps Average Out: 249.55 Kpps Current Out: 257.08 Kpps

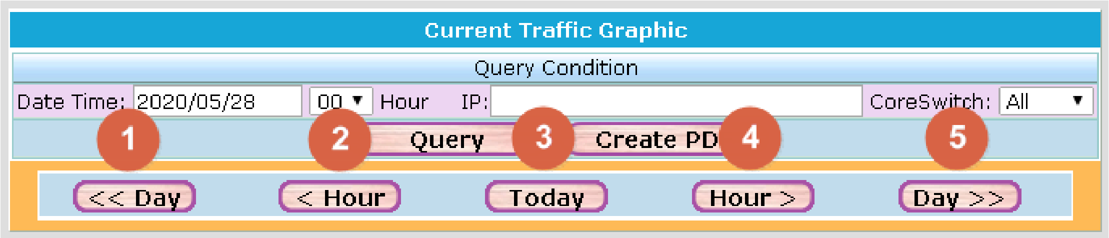
Figure 38 – The 24-hour report

Possible condition types are described below:

- **Date Time:** You can change this report to a different start time.
- **IP:** You can specify an internal IP address.
- **Core Switch:** You can specify the data source for the report.

You can also change the start time by clicking the following button.

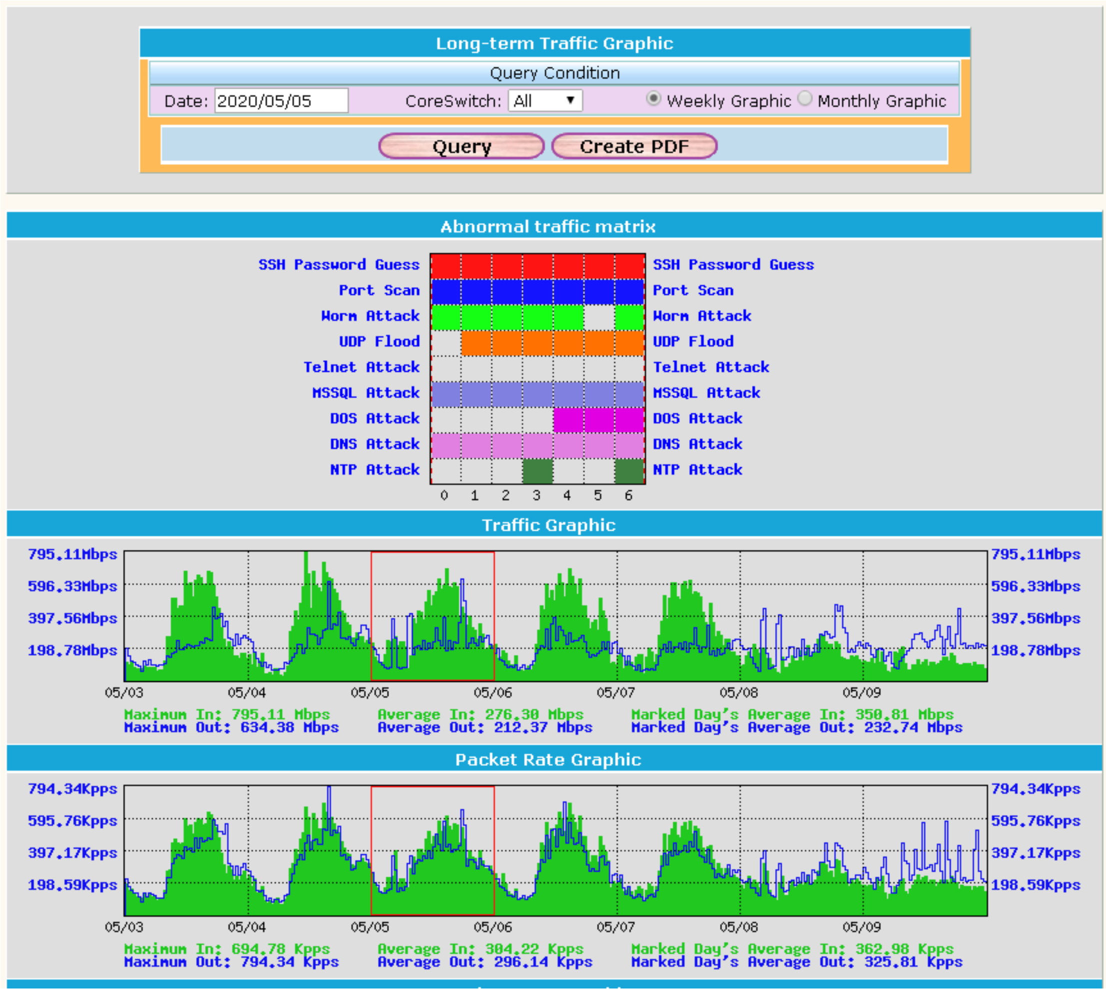
#	Description
1	Set the start time to the previous day
2	Set the start time to the previous hour
3	Set the start time to the current day
4	Set the start time to the next hour
5	Set the start time to the next day



Date Time: 2020/05/28 00 Hour IP: CoreSwitch: All

Long Term Graphic:

Flowwatch can provide the monthly and yearly statistics and graph to the administrator. You can export the results of a report to a PDF file by clicking the **Create PDF** button. For the weekly date-time axes, we use numbers to display the weekday (0-6, 0 being Sunday).



Date: 2020/05/05 CoreSwitch: All ● Weekly Graphic ○ Monthly Graphic

	0	1	2	3	4	5	6	
SSH Password Guess	■	■	■	■	■	■	■	SSH Password Guess
Port Scan	■	■	■	■	■	■	■	Port Scan
Worm Attack	■	■	■	■	■		■	Worm Attack
UDP Flood		■	■	■	■	■	■	UDP Flood
Telnet Attack								Telnet Attack
MSSQL Attack	■	■	■	■	■	■	■	MSSQL Attack
DOS Attack					■	■	■	DOS Attack
DNS Attack	■	■	■	■	■	■	■	DNS Attack
NTP Attack				■			■	NTP Attack

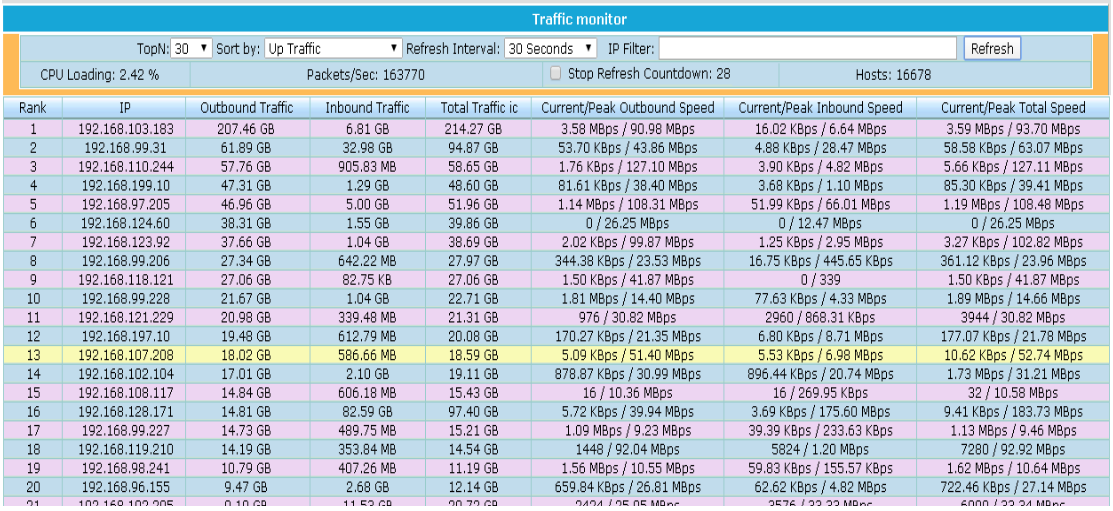
Maximum In: 795.11 Mbps
Maximum Out: 634.38 Mbps
Average In: 276.30 Mbps
Average Out: 212.37 Mbps
Marked Day's Average In: 350.81 Mbps
Marked Day's Average Out: 232.74 Mbps

Maximum In: 694.78 Kpps
Maximum Out: 794.34 Kpps
Average In: 304.22 Kpps
Average Out: 296.14 Kpps
Marked Day's Average In: 362.98 Kpps
Marked Day's Average Out: 325.81 Kpps

Figure 39 – The weekly graph

Traffic Monitor:

This feature allows you to monitor the network traffic of each IP address. The input field : '**IP Filter**' runs the fuzzy search.



Traffic monitor

TopN: 30 ▾ Sort by: Up Traffic ▾ Refresh Interval: 30 Seconds ▾ IP Filter: Refresh

CPU Loading: 2.42 % | Packets/Sec: 163770 | □ Stop Refresh Countdown: 28 | Hosts: 16678

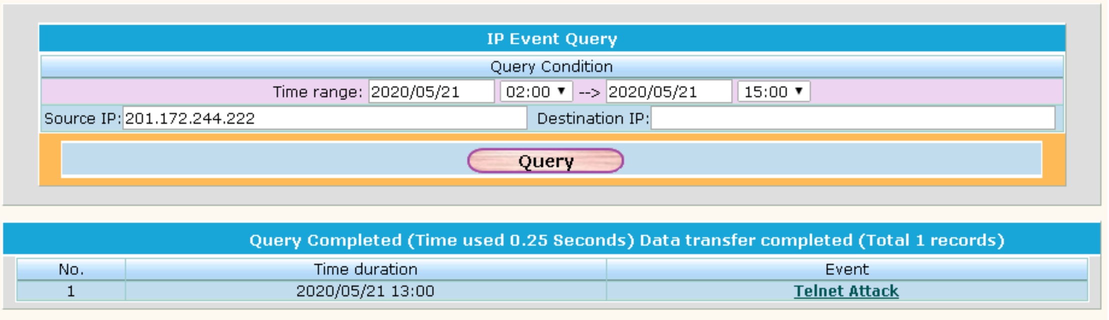
Rank	IP	Outbound Traffic	Inbound Traffic	Total Traffic ic	Current/Peak Outbound Speed	Current/Peak Inbound Speed	Current/Peak Total Speed
1	192.168.103.183	207.46 GB	6.81 GB	214.27 GB	3.58 MBps / 90.98 MBps	16.02 KBps / 6.64 MBps	3.59 MBps / 93.70 MBps
2	192.168.99.31	61.89 GB	32.98 GB	94.87 GB	53.70 KBps / 43.86 MBps	4.88 KBps / 28.47 MBps	58.58 KBps / 63.07 MBps
3	192.168.110.244	57.76 GB	905.83 MB	58.65 GB	1.76 KBps / 127.10 MBps	3.90 KBps / 4.82 MBps	5.66 KBps / 127.11 MBps
4	192.168.199.10	47.31 GB	1.29 GB	48.60 GB	81.61 KBps / 38.40 MBps	3.68 KBps / 1.10 MBps	85.30 KBps / 39.41 MBps
5	192.168.97.205	46.96 GB	5.00 GB	51.96 GB	1.14 MBps / 108.31 MBps	51.99 KBps / 66.01 MBps	1.19 MBps / 108.48 MBps
6	192.168.124.60	38.31 GB	1.55 GB	39.86 GB	0 / 26.25 MBps	0 / 12.47 MBps	0 / 26.25 MBps
7	192.168.123.92	37.66 GB	1.04 GB	38.69 GB	2.02 KBps / 99.87 MBps	1.25 KBps / 2.95 MBps	3.27 KBps / 102.82 MBps
8	192.168.99.206	27.34 GB	642.22 MB	27.97 GB	344.38 KBps / 23.53 MBps	16.75 KBps / 445.65 KBps	361.12 KBps / 23.96 MBps
9	192.168.118.121	27.06 GB	82.75 KB	27.06 GB	1.50 KBps / 41.87 MBps	0 / 339	1.50 KBps / 41.87 MBps
10	192.168.99.228	21.67 GB	1.04 GB	22.71 GB	1.81 MBps / 14.40 MBps	77.63 KBps / 4.33 MBps	1.89 MBps / 14.66 MBps
11	192.168.121.229	20.98 GB	339.48 MB	21.31 GB	976 / 30.82 MBps	2960 / 868.31 KBps	3944 / 30.82 MBps
12	192.168.197.10	19.48 GB	612.79 MB	20.08 GB	170.27 KBps / 21.35 MBps	6.80 KBps / 8.71 MBps	177.07 KBps / 21.78 MBps
13	192.168.107.208	18.02 GB	586.66 MB	18.59 GB	5.09 KBps / 51.40 MBps	5.53 KBps / 6.98 MBps	10.62 KBps / 52.74 MBps
14	192.168.102.104	17.01 GB	2.10 GB	19.11 GB	878.87 KBps / 30.99 MBps	896.44 KBps / 20.74 MBps	1.73 MBps / 31.21 MBps
15	192.168.108.117	14.84 GB	606.18 MB	15.43 GB	16 / 10.36 MBps	16 / 269.95 KBps	32 / 10.58 MBps
16	192.168.128.171	14.81 GB	82.59 GB	97.40 GB	5.72 KBps / 39.94 MBps	3.69 KBps / 175.60 MBps	9.41 KBps / 183.73 MBps
17	192.168.99.227	14.73 GB	489.75 MB	15.21 GB	1.09 MBps / 9.23 MBps	39.39 KBps / 233.63 KBps	1.13 MBps / 9.46 MBps
18	192.168.119.210	14.19 GB	353.84 MB	14.54 GB	1448 / 92.04 MBps	5824 / 1.20 MBps	7280 / 92.92 MBps
19	192.168.98.241	10.79 GB	407.26 MB	11.19 GB	1.56 MBps / 10.55 MBps	59.83 KBps / 155.57 KBps	1.62 MBps / 10.64 MBps
20	192.168.96.155	9.47 GB	2.68 GB	12.14 GB	659.84 KBps / 26.81 MBps	62.62 KBps / 4.82 MBps	722.46 KBps / 27.14 MBps
21	192.168.102.205	9.10 GB	11.53 GB	20.72 GB	2424 / 25.05 MBps	3576 / 33.33 MBps	6000 / 33.34 MBps

Figure – The Traffic Monitor

IP Event Query:

Sometimes you may want to find out the event for a specific IP address. You can enter the IP address into the ‘Source IP’ or ‘Destination IP’ field.

Note: You have to fill in at least one field.



IP Event Query

Query Condition

Time range: 2020/05/21 02:00 ▾ --> 2020/05/21 15:00 ▾

Source IP: 201.172.244.222 Destination IP:

Query

Query Completed (Time used 0.25 Seconds) Data transfer completed (Total 1 records)

No.	Time duration	Event
1	2020/05/21 13:00	Telnet Attack

Figure 40 – Generate the event report for the particular IP address

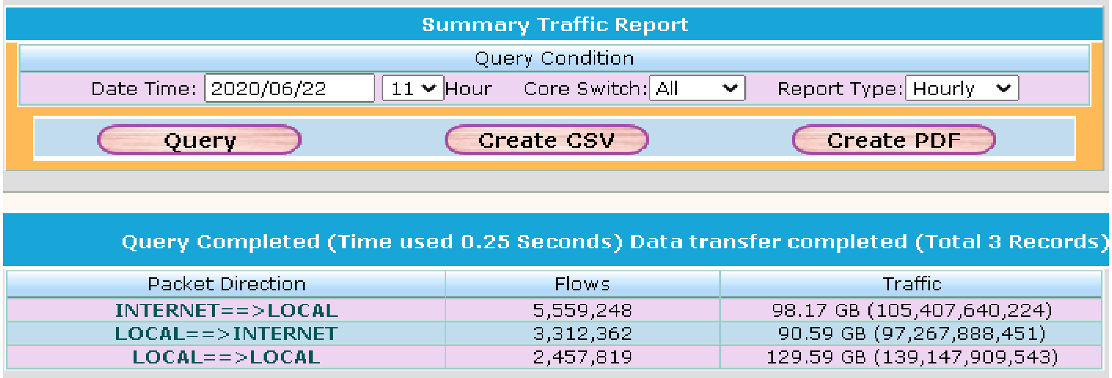
Report

The Flowwatch can provide kinds of report. You can export the results of a report to a PDF or CSV file. The flowwatch can provide the network traffic usage report on an hourly, daily, weekly, monthly and yearly basis.

Note: The trial version can only display the hourly, daily and weekly report. In the hourly report, the trial version can only list the first 10 results. In the daily report, the trial version can only display the first 30 results.

Traffic Summary:

The Flowwatch system can provide a network traffic usage report to the administrator. The administrator can also read the drill through report for the traffic usage of each network service. These report can be exported to CSV / PDF file by clicking the **Create CSV/Create PDF** button



Summary Traffic Report

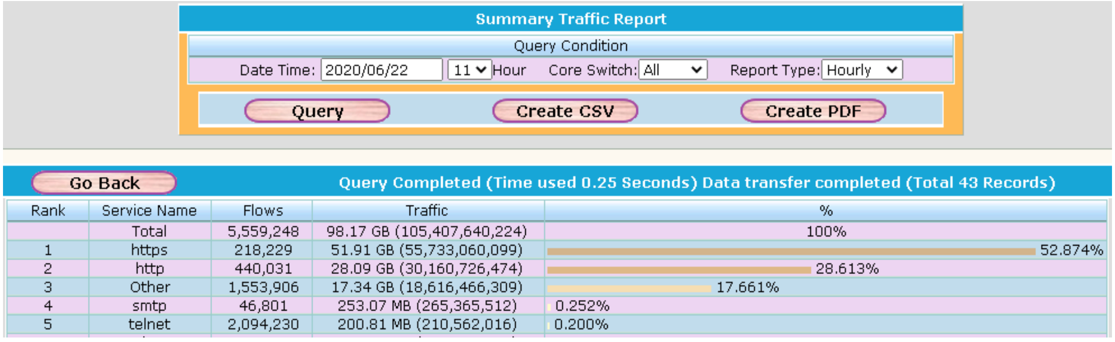
Query Condition

Date Time: 2020/06/22 11 Hour Core Switch: All Report Type: Hourly

Query Completed (Time used 0.25 Seconds) Data transfer completed (Total 3 Records)

Packet Direction	Flows	Traffic
INTERNET==>LOCAL	5,559,248	98.17 GB (105,407,640,224)
LOCAL==>INTERNET	3,312,362	90.59 GB (97,267,888,451)
LOCAL==>LOCAL	2,457,819	129.59 GB (139,147,909,543)

Figure 41 – The traffic usage report



Summary Traffic Report

Query Condition

Date Time: 2020/06/22 11 Hour Core Switch: All Report Type: Hourly

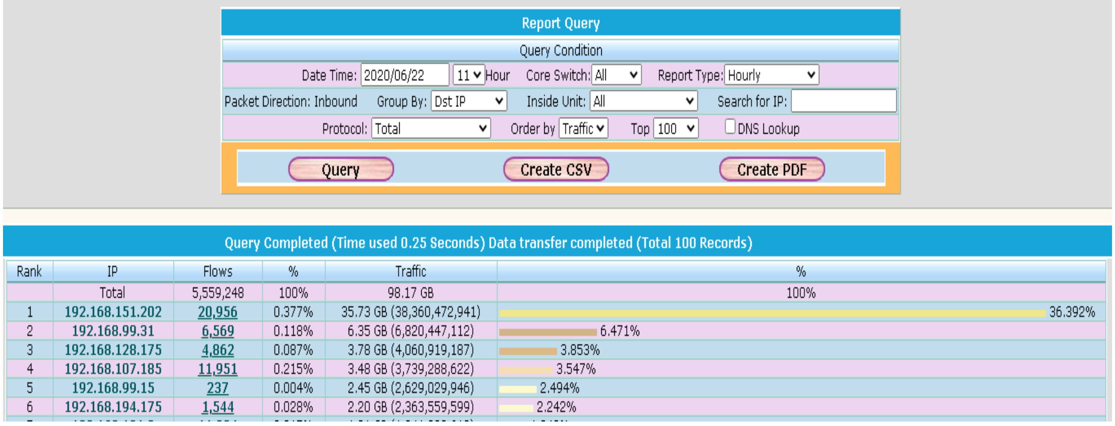
Query Completed (Time used 0.25 Seconds) Data transfer completed (Total 43 Records)

Rank	Service Name	Flows	Traffic	%
	Total	5,559,248	98.17 GB (105,407,640,224)	100%
1	https	218,229	51.91 GB (55,733,060,099)	52.874%
2	http	440,031	28.09 GB (30,160,726,474)	28.613%
3	Other	1,553,906	17.34 GB (18,616,466,309)	17.661%
4	smtp	46,801	253.07 MB (265,365,512)	0.252%
5	telnet	2,094,230	200.81 MB (210,562,016)	0.200%

Figure 42 – The inbound traffic usage of each network service

Inbound Dst. :

The administrator can use the cross filter to create an inbound network traffic report which grouped by the destination IP address.



Report Query

Query Condition

Date Time: 2020/06/22 11 Hour Core Switch: All Report Type: Hourly

Packet Direction: Inbound Group By: Dst IP Inside Unit: All Search for IP:

Protocol: Total Order by Traffic Top 100 ☐ DNS Lookup

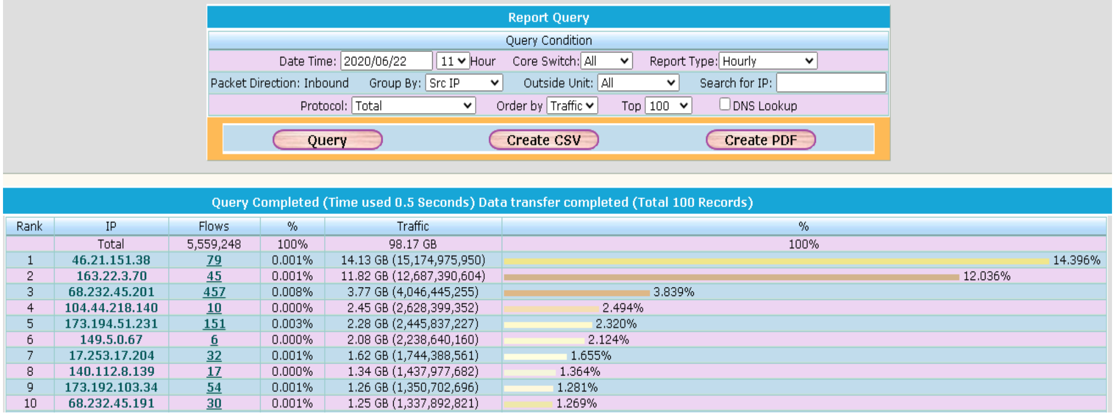
Query Completed (Time used 0.25 Seconds) Data transfer completed (Total 100 Records)

Rank	IP	Flows	%	Traffic	%
	Total	5,559,248	100%	98.17 GB	100%
1	192.168.151.202	20,956	0.377%	35.73 GB (38,360,472,941)	36.392%
2	192.168.99.31	6,569	0.118%	6.35 GB (6,820,447,112)	6.471%
3	192.168.128.175	4,862	0.087%	3.78 GB (4,060,919,187)	3.853%
4	192.168.107.185	11,951	0.215%	3.48 GB (3,739,288,622)	3.547%
5	192.168.99.15	237	0.004%	2.45 GB (2,629,029,946)	2.494%
6	192.168.194.175	1,544	0.028%	2.20 GB (2,363,559,599)	2.242%

Figure 43 – The inbound traffic report

Inbound Src. :

The administrator can use the cross filter to create an inbound network traffic report which grouped by the source IP address.



Date Time: 2020/06/22 11 Hour Core Switch: All Report Type: Hourly

Packet Direction: Inbound Group By: Src IP Outside Unit: All Search for IP:

Protocol: Total Order by Traffic Top 100 □ DNS Lookup

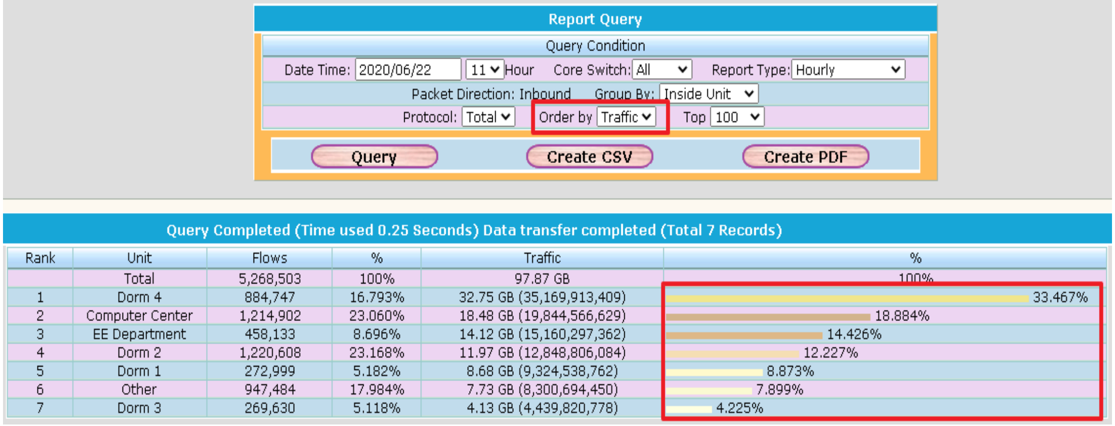
Query Completed (Time used 0.5 Seconds) Data transfer completed (Total 100 Records)

Rank	IP	Flows	%	Traffic	%
	Total	5,559,248	100%	98.17 GB	100%
1	46.21.151.38	79	0.001%	14.13 GB (15,174,975,950)	14.396%
2	163.22.3.70	45	0.001%	11.82 GB (12,687,390,604)	12.036%
3	68.232.45.201	457	0.008%	3.77 GB (4,046,445,255)	3.839%
4	104.44.218.140	10	0.000%	2.45 GB (2,628,399,352)	2.494%
5	173.194.51.231	151	0.003%	2.28 GB (2,445,837,227)	2.320%
6	149.5.0.67	6	0.000%	2.08 GB (2,238,640,160)	2.124%
7	17.253.17.204	32	0.001%	1.62 GB (1,744,388,561)	1.655%
8	140.112.8.139	17	0.000%	1.34 GB (1,437,977,682)	1.364%
9	173.192.103.34	54	0.001%	1.26 GB (1,350,702,696)	1.281%
10	68.232.45.191	30	0.001%	1.25 GB (1,337,892,821)	1.269%

Figure 44 – The inbound traffic report

Inbound Unit:

The administrator can use the cross filter to check the inbound network traffic of each unit.



Date Time: 2020/06/22 11 Hour Core Switch: All Report Type: Hourly

Packet Direction: Inbound Group By: Inside Unit

Protocol: Total Order by Traffic Top 100

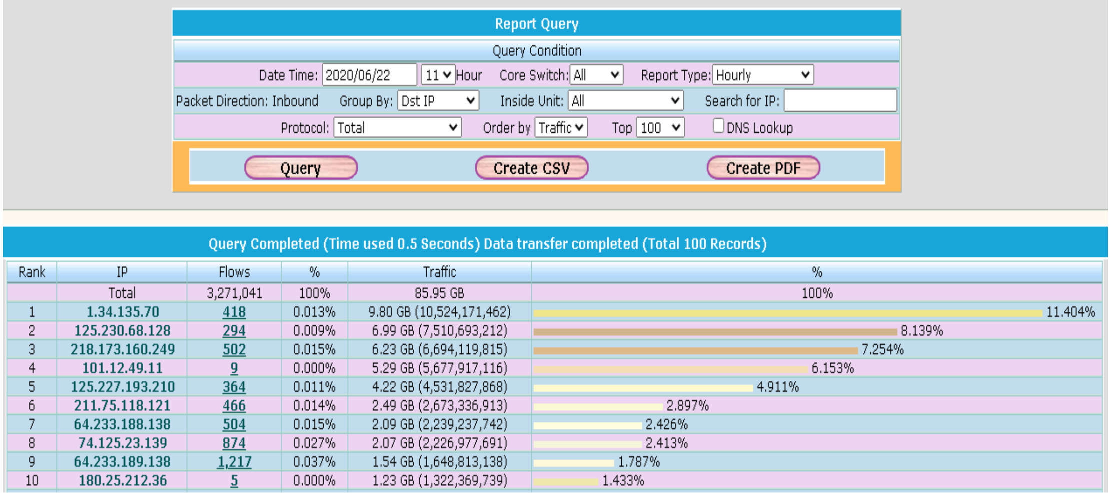
Query Completed (Time used 0.25 Seconds) Data transfer completed (Total 7 Records)

Rank	Unit	Flows	%	Traffic	%
	Total	5,268,503	100%	97.87 GB	100%
1	Dorm 4	884,747	16.793%	32.75 GB (35,169,913,409)	33.467%
2	Computer Center	1,214,902	23.060%	18.48 GB (19,844,566,629)	18.884%
3	EE Department	458,133	8.696%	14.12 GB (15,160,297,362)	14.426%
4	Dorm 2	1,220,608	23.168%	11.97 GB (12,848,806,084)	12.227%
5	Dorm 1	272,999	5.182%	8.68 GB (9,324,538,762)	8.873%
6	Other	947,484	17.984%	7.73 GB (8,300,694,450)	7.899%
7	Dorm 3	269,630	5.118%	4.13 GB (4,439,820,778)	4.225%

Figure 45 – The inbound traffic report of each unit

Outbound Dst. :

The administrator can use the cross filter to create an outbound network traffic report which grouped by the destination IP address.



Report Query

Query Condition

Date Time: 2020/06/22 11 Hour Core Switch: All Report Type: Hourly

Packet Direction: Inbound Group By: Dst IP Inside Unit: All Search for IP:

Protocol: Total Order by Traffic Top 100 □DNS Lookup

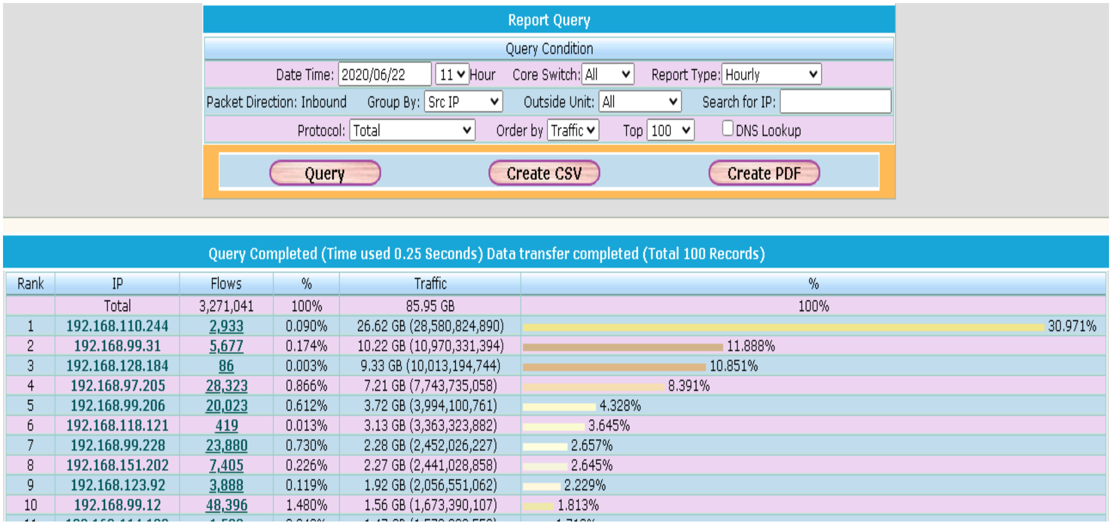
Query Completed (Time used 0.5 Seconds) Data transfer completed (Total 100 Records)

Rank	IP	Flows	%	Traffic	%
	Total	3,271,041	100%	85.95 GB	100%
1	1.34.135.70	418	0.013%	9.80 GB (10,524,171,462)	11.404%
2	125.230.68.128	294	0.009%	6.99 GB (7,510,693,212)	8.139%
3	218.173.160.249	502	0.015%	6.23 GB (6,694,119,815)	7.254%
4	101.12.49.11	9	0.000%	5.29 GB (5,677,917,116)	6.153%
5	125.227.193.210	364	0.011%	4.22 GB (4,531,827,868)	4.911%
6	211.75.118.121	466	0.014%	2.49 GB (2,673,336,913)	2.897%
7	64.233.188.138	504	0.015%	2.09 GB (2,239,237,742)	2.426%
8	74.125.23.139	874	0.027%	2.07 GB (2,226,977,691)	2.413%
9	64.233.189.138	1,217	0.037%	1.54 GB (1,648,813,138)	1.787%
10	180.25.212.36	5	0.000%	1.23 GB (1,322,369,739)	1.433%

Figure 46 – The outbound traffic report

Outbound Src. :

The administrator can use the cross filter to create an outbound network traffic report which grouped by the source IP address.



Report Query

Query Condition

Date Time: 2020/06/22 11 Hour Core Switch: All Report Type: Hourly

Packet Direction: Inbound Group By: Src IP Outside Unit: All Search for IP:

Protocol: Total Order by Traffic Top 100 □DNS Lookup

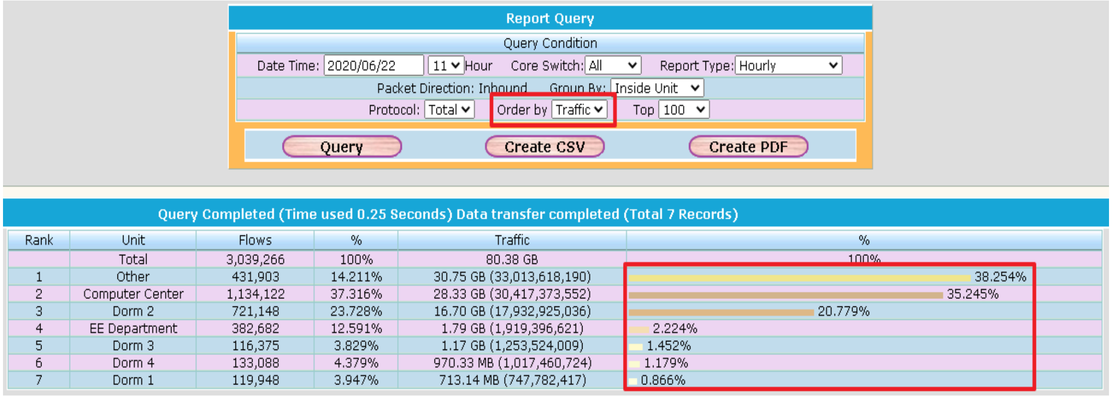
Query Completed (Time used 0.25 Seconds) Data transfer completed (Total 100 Records)

Rank	IP	Flows	%	Traffic	%
	Total	3,271,041	100%	85.95 GB	100%
1	192.168.110.244	2,933	0.090%	26.62 GB (28,580,824,890)	30.971%
2	192.168.99.31	5,677	0.174%	10.22 GB (10,970,331,394)	11.888%
3	192.168.128.184	86	0.003%	9.33 GB (10,013,194,744)	10.851%
4	192.168.97.205	28,323	0.866%	7.21 GB (7,743,735,058)	8.391%
5	192.168.99.206	20,023	0.612%	3.72 GB (3,994,100,761)	4.328%
6	192.168.118.121	419	0.013%	3.13 GB (3,363,323,882)	3.645%
7	192.168.99.228	23,880	0.730%	2.28 GB (2,452,026,227)	2.657%
8	192.168.151.202	7,405	0.226%	2.27 GB (2,441,028,858)	2.645%
9	192.168.123.92	3,888	0.119%	1.92 GB (2,056,551,062)	2.229%
10	192.168.99.12	48,396	1.480%	1.56 GB (1,673,390,107)	1.813%

Figure 47 – The outbound traffic report

Outbound Unit:

The administrator can use the cross filter to check the outbound network traffic of each unit.



Report Query

Query Condition

Date Time: 2020/06/22 | 11 Hour | Core Switch: All | Report Type: Hourly

Packet Direction: Inbound | Group By: Inside Unit

Protocol: Total | Order by Traffic | Top 100

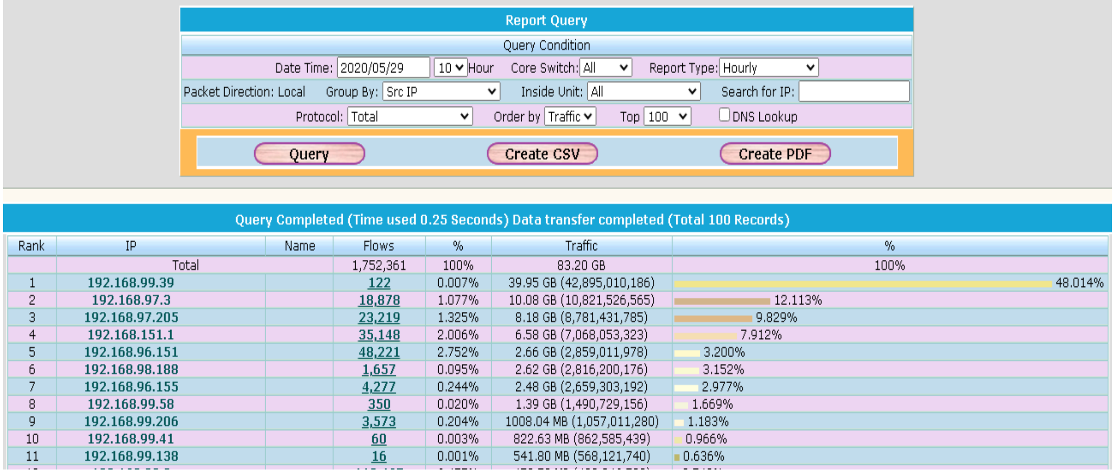
Query Completed (Time used 0.25 Seconds) Data transfer completed (Total 7 Records)

Rank	Unit	Flows	%	Traffic	%
	Total	3,039,266	100%	80.38 GB	100%
1	Other	431,903	14.211%	30.75 GB (33,013,618,190)	38.254%
2	Computer Center	1,134,122	37.316%	28.33 GB (30,417,373,552)	35.245%
3	Dorm 2	721,148	23.728%	16.70 GB (17,932,925,036)	20.779%
4	EE Department	382,682	12.591%	1.79 GB (1,919,396,621)	2.224%
5	Dorm 3	116,375	3.829%	1.17 GB (1,253,524,009)	1.452%
6	Dorm 4	133,088	4.379%	970.33 MB (1,017,460,724)	1.179%
7	Dorm 1	119,948	3.947%	713.14 MB (747,782,417)	0.866%

Figure 48 – The outbound traffic report of each unit

Local Traffic:

The administrator can use the cross filter to check the internal network traffic.



Report Query

Query Condition

Date Time: 2020/05/29 | 10 Hour | Core Switch: All | Report Type: Hourly

Packet Direction: Local | Group By: Src IP | Inside Unit: All | Search for IP:

Protocol: Total | Order by Traffic | Top 100 | □ DNS Lookup

Query Completed (Time used 0.25 Seconds) Data transfer completed (Total 100 Records)

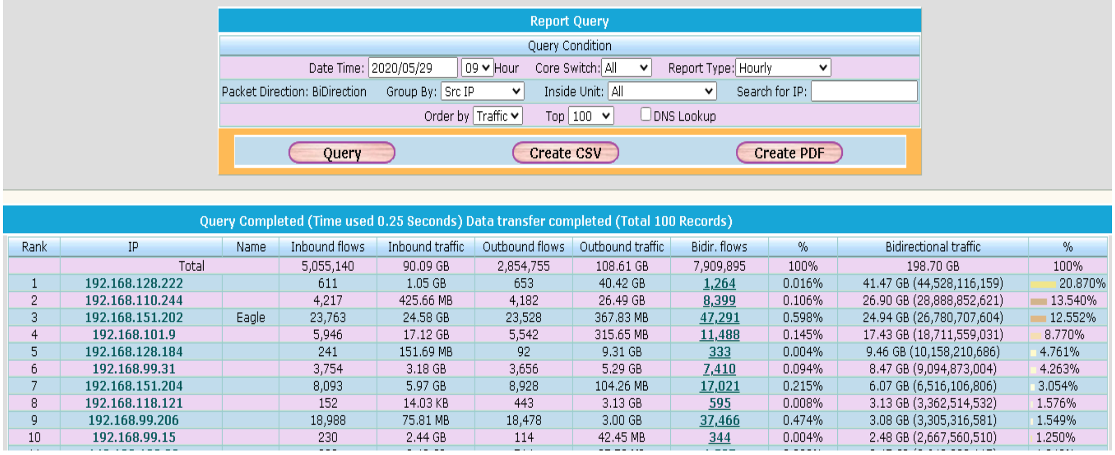
Rank	IP	Name	Flows	%	Traffic	%
	Total		1,752,361	100%	83.20 GB	100%
1	192.168.99.39		122	0.007%	39.95 GB (42,895,010,186)	48.014%
2	192.168.97.3		18,878	1.077%	10.08 GB (10,821,526,565)	12.113%
3	192.168.97.205		23,219	1.325%	8.18 GB (8,781,431,785)	9.829%
4	192.168.151.1		35,148	2.006%	6.58 GB (7,068,053,323)	7.912%
5	192.168.96.151		48,221	2.752%	2.66 GB (2,859,011,978)	3.200%
6	192.168.98.188		1,657	0.095%	2.62 GB (2,816,200,176)	3.152%
7	192.168.96.155		4,277	0.244%	2.48 GB (2,659,303,192)	2.977%
8	192.168.99.58		350	0.020%	1.39 GB (1,490,729,156)	1.669%
9	192.168.99.206		3,573	0.204%	1008.04 MB (1,057,011,280)	1.183%
10	192.168.99.41		60	0.003%	822.63 MB (862,585,439)	0.966%
11	192.168.99.138		16	0.001%	541.80 MB (568,121,740)	0.636%

Figure 49 – The report of internal network traffic

Note: The ‘Name’ is custom field.

BiDirection Traffic:

The administrator can use the cross filter to check the bidirectional traffic.



Report Query

Query Condition

Date Time: 2020/05/29 | 09 Hour | Core Switch: All | Report Type: Hourly

Packet Direction: BiDirection | Group By: Src IP | Inside Unit: All | Search for IP:

Order by Traffic | Top 100 | □ DNS Lookup

Query Completed (Time used 0.25 Seconds) Data transfer completed (Total 100 Records)

Rank	IP	Name	Inbound flows	Inbound traffic	Outbound flows	Outbound traffic	Bidir. flows	%	Bidirectional traffic	%
	Total		5,055,140	90.09 GB	2,854,755	108.61 GB	7,909,895	100%	198.70 GB	100%
1	192.168.128.222		611	1.05 GB	653	40.42 GB	1,264	0.016%	41.47 GB (44,528,116,159)	20.870%
2	192.168.110.244		4,217	425.66 MB	4,182	26.49 GB	8,399	0.106%	26.90 GB (28,888,852,621)	13.540%
3	192.168.151.202	Eagle	23,763	24.58 GB	23,528	367.83 MB	47,291	0.598%	24.94 GB (26,780,707,604)	12.552%
4	192.168.101.9		5,946	17.12 GB	5,542	315.65 MB	11,488	0.145%	17.43 GB (18,711,559,031)	8.770%
5	192.168.128.184		241	151.69 MB	92	9.31 GB	333	0.004%	9.46 GB (10,158,210,686)	4.761%
6	192.168.99.31		3,754	3.18 GB	3,656	5.29 GB	7,410	0.094%	8.47 GB (9,094,873,004)	4.263%
7	192.168.151.204		8,093	5.97 GB	8,928	104.26 MB	17,021	0.215%	6.07 GB (6,516,106,806)	3.054%
8	192.168.118.121		152	14.03 KB	443	3.13 GB	595	0.008%	3.13 GB (3,362,514,532)	1.576%
9	192.168.99.206		18,988	75.81 MB	18,478	3.00 GB	37,466	0.474%	3.08 GB (3,305,316,581)	1.549%
10	192.168.99.15		230	2.44 GB	114	42.45 MB	344	0.004%	2.48 GB (2,667,560,510)	1.250%

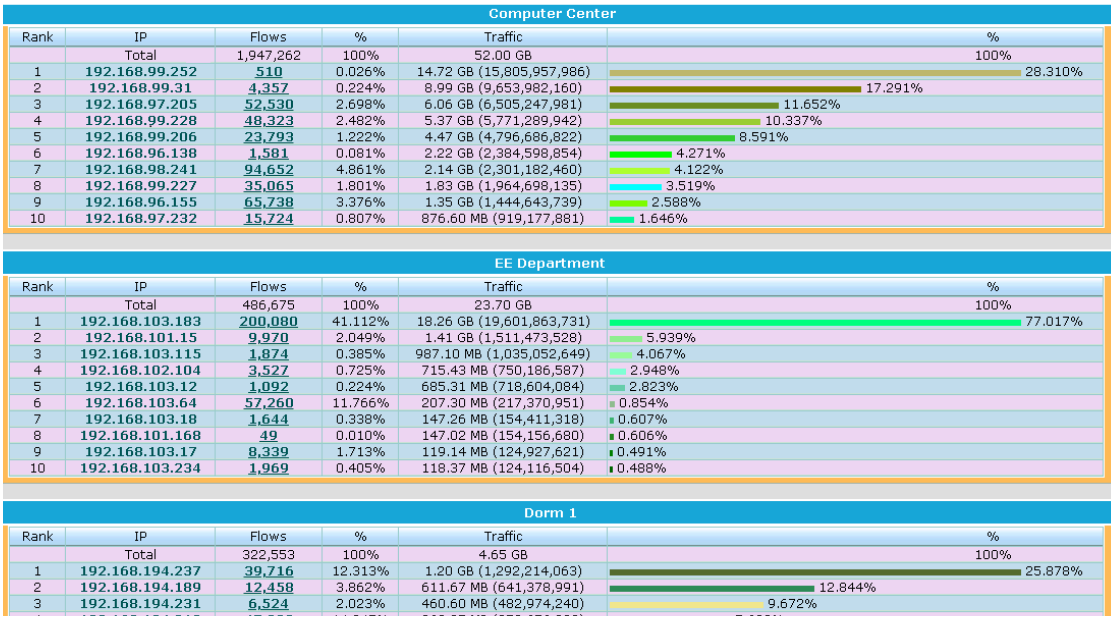
Figure 50 – The report of bidirectional traffic

Note: The ‘Name’ is custom field.

Top N Per Unit:

The administrator can check the top N lists of the unit. If you do not set any unit, all data will be regarded to the unit: Other

For more about setting the unit, refer to this section.



Computer Center

Rank	IP	Flows	%	Traffic	%
	Total	1,947,262	100%	52.00 GB	100%
1	192.168.99.252	510	0.026%	14.72 GB (15,805,957,986)	28.310%
2	192.168.99.31	4,357	0.224%	8.99 GB (9,653,982,160)	17.291%
3	192.168.97.205	52,530	2.698%	6.06 GB (6,505,247,981)	11.652%
4	192.168.99.228	48,323	2.482%	5.37 GB (5,771,289,942)	10.337%
5	192.168.99.206	23,793	1.222%	4.47 GB (4,796,686,822)	8.591%
6	192.168.96.138	1,581	0.081%	2.22 GB (2,384,598,854)	4.271%
7	192.168.98.241	94,652	4.861%	2.14 GB (2,301,182,460)	4.122%
8	192.168.99.227	35,065	1.801%	1.83 GB (1,964,698,135)	3.519%
9	192.168.96.155	65,738	3.376%	1.35 GB (1,444,643,739)	2.588%
10	192.168.97.232	15,724	0.807%	876.60 MB (919,177,881)	1.646%

EE Department

Rank	IP	Flows	%	Traffic	%
	Total	486,675	100%	23.70 GB	100%
1	192.168.103.183	200,080	41.112%	18.26 GB (19,601,863,731)	77.017%
2	192.168.101.15	9,970	2.049%	1.41 GB (1,511,473,528)	5.939%
3	192.168.103.115	1,874	0.385%	987.10 MB (1,035,052,649)	4.067%
4	192.168.102.104	3,527	0.725%	715.43 MB (750,186,587)	2.948%
5	192.168.103.12	1,092	0.224%	685.31 MB (718,604,084)	2.823%
6	192.168.103.64	57,260	11.766%	207.30 MB (217,370,951)	0.854%
7	192.168.103.18	1,644	0.338%	147.26 MB (154,411,318)	0.607%
8	192.168.101.168	49	0.010%	147.02 MB (154,156,680)	0.606%
9	192.168.103.17	8,339	1.713%	119.14 MB (124,927,621)	0.491%
10	192.168.103.234	1,969	0.405%	118.37 MB (124,116,504)	0.488%

Dorm 1

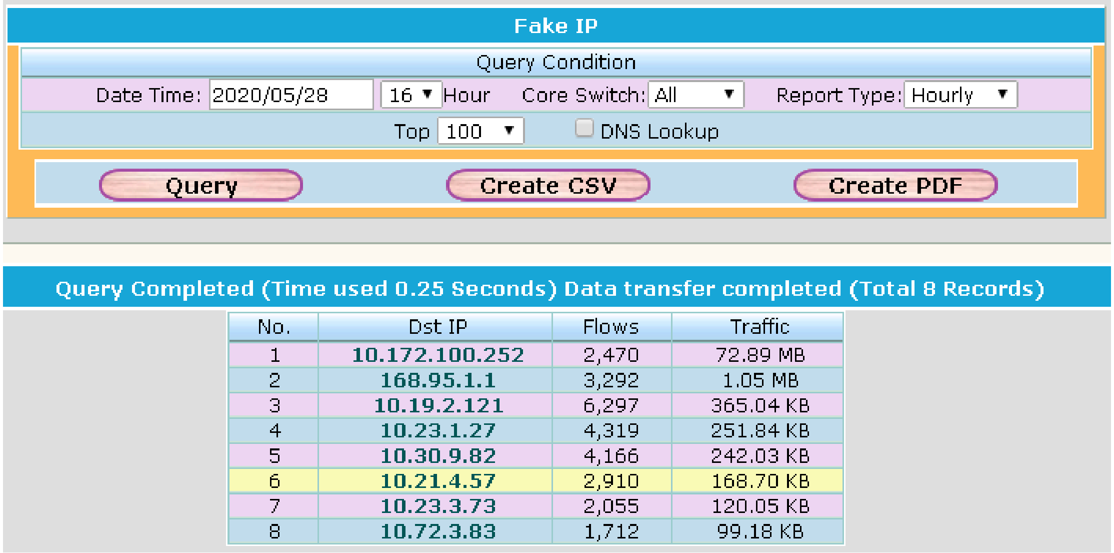
Rank	IP	Flows	%	Traffic	%
	Total	322,553	100%	4.65 GB	100%
1	192.168.194.237	39,716	12.313%	1.20 GB (1,292,214,063)	25.878%
2	192.168.194.189	12,458	3.862%	611.67 MB (641,378,991)	12.844%
3	192.168.194.231	6,524	2.023%	460.60 MB (482,974,240)	9.672%

Figure 51 – Top N report of each unit

Note: The **Protocol** filter will be effectively useless when the **Packet Direction** is set to Bidirection.

Fake IP:

Generally, you should find the local IP address in the source IP field or destination IP field. If the system detect the IP in either field, it means someone might spoof an IP address. You can also export the report to CSV / PDF file by clicking the **Create CSV/Create PDF** button.



Fake IP

Query Condition

Date Time: 2020/05/28 16 Hour Core Switch: All Report Type: Hourly

Top 100 □ DNS Lookup

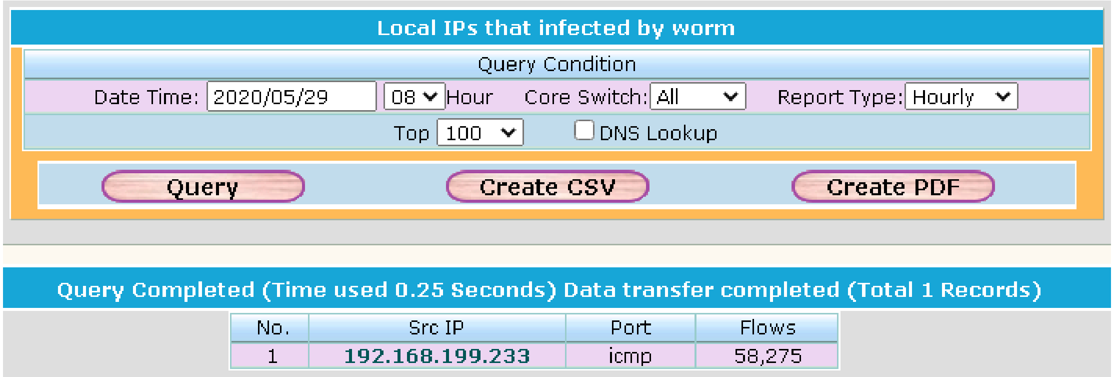
Query Completed (Time used 0.25 Seconds) Data transfer completed (Total 8 Records)

No.	Dst IP	Flows	Traffic
1	10.172.100.252	2,470	72.89 MB
2	168.95.1.1	3,292	1.05 MB
3	10.19.2.121	6,297	365.04 KB
4	10.23.1.27	4,319	251.84 KB
5	10.30.9.82	4,166	242.03 KB
6	10.21.4.57	2,910	168.70 KB
7	10.23.3.73	2,055	120.05 KB
8	10.72.3.83	1,712	99.18 KB

Figure 52 – The report of fake IP

Worm Report:

You can use the cross filter to find the worm attack records that you need in a report. You can also export the report to CSV / PDF file by clicking the **Create CSV/Create PDF** button.



Local IPs that infected by worm

Query Condition

Date Time: 2020/05/29 08 Hour Core Switch: All Report Type: Hourly

Top 100 □ DNS Lookup

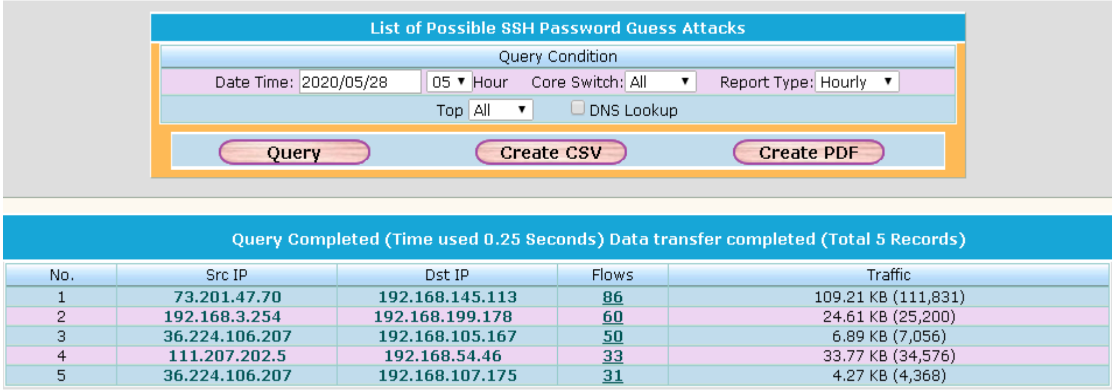
Query Completed (Time used 0.25 Seconds) Data transfer completed (Total 1 Records)

No.	Src IP	Port	Flows
1	192.168.199.233	icmp	58,275

Figure 53 – The report of worm attack

SSH Passwd Guess:

You can use the cross filter to find the SSH password guessing attack records that you need in a report. You can also export the report to CSV / PDF file by clicking the **Create CSV/Create PDF** button.



List of Possible SSH Password Guess Attacks

Query Condition

Date Time: 2020/05/28 05 Hour Core Switch: All Report Type: Hourly

Top All □ DNS Lookup

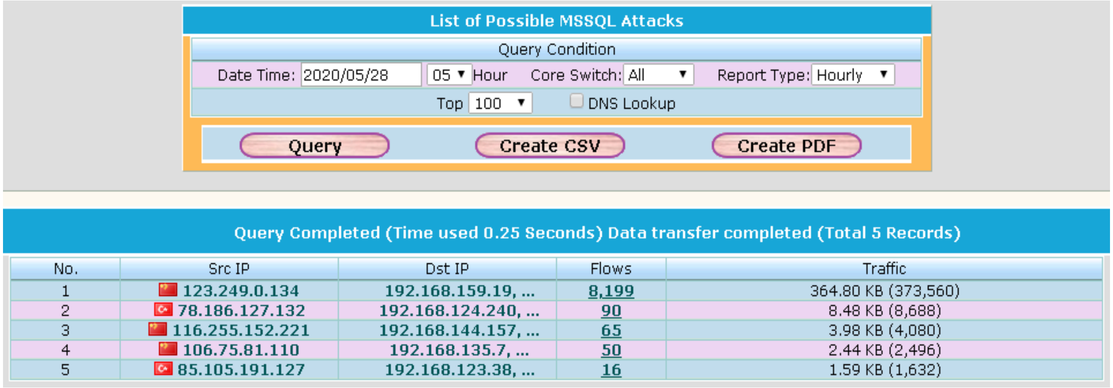
Query Completed (Time used 0.25 Seconds) Data transfer completed (Total 5 Records)

No.	Src IP	Dst IP	Flows	Traffic
1	73.201.47.70	192.168.145.113	86	109.21 KB (111,831)
2	192.168.3.254	192.168.199.178	60	24.61 KB (25,200)
3	36.224.106.207	192.168.105.167	50	6.89 KB (7,056)
4	111.207.202.5	192.168.54.46	33	33.77 KB (34,576)
5	36.224.106.207	192.168.107.175	31	4.27 KB (4,368)

Figure 54 – The report of SSH password guessing attack

MSSQL Attack:

You can use the cross filter to find the MSSQL attack records that you need in a report. You can also export the report to CSV / PDF file by clicking the **Create CSV/Create PDF** button.



List of Possible MSSQL Attacks

Query Condition

Date Time: 2020/05/28 05 Hour Core Switch: All Report Type: Hourly

Top 100 □ DNS Lookup

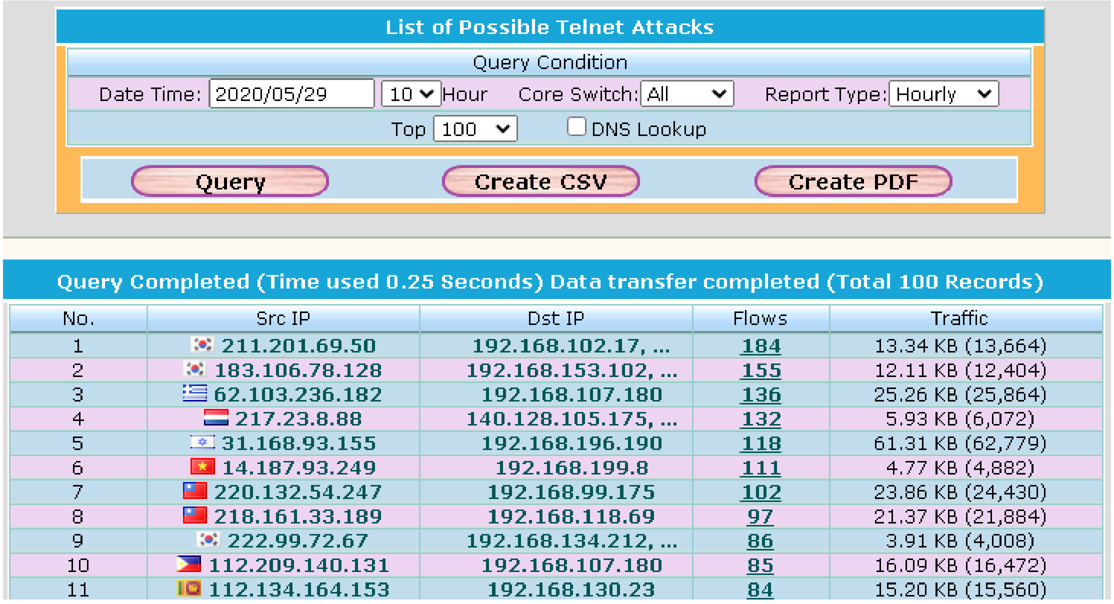
Query Completed (Time used 0.25 Seconds) Data transfer completed (Total 5 Records)

No.	Src IP	Dst IP	Flows	Traffic
1	🇨🇳 123.249.0.134	192.168.159.19, ...	8,199	364.80 KB (373,560)
2	🇹🇷 78.186.127.132	192.168.124.240, ...	90	8.48 KB (8,688)
3	🇨🇳 116.255.152.221	192.168.144.157, ...	65	3.98 KB (4,080)
4	🇨🇳 106.75.81.110	192.168.135.7, ...	50	2.44 KB (2,496)
5	🇹🇷 85.105.191.127	192.168.123.38, ...	16	1.59 KB (1,632)

Figure 55 – The report of MSSQL attack

Telnet Attack:

You can use the cross filter to find the Telnet attack records that you need in a report. You can also export the report to CSV / PDF file by clicking the **Create CSV/Create PDF** button.



List of Possible Telnet Attacks

Query Condition

Date Time: 2020/05/29 | 10 Hour | Core Switch: All | Report Type: Hourly

Top 100 | □ DNS Lookup

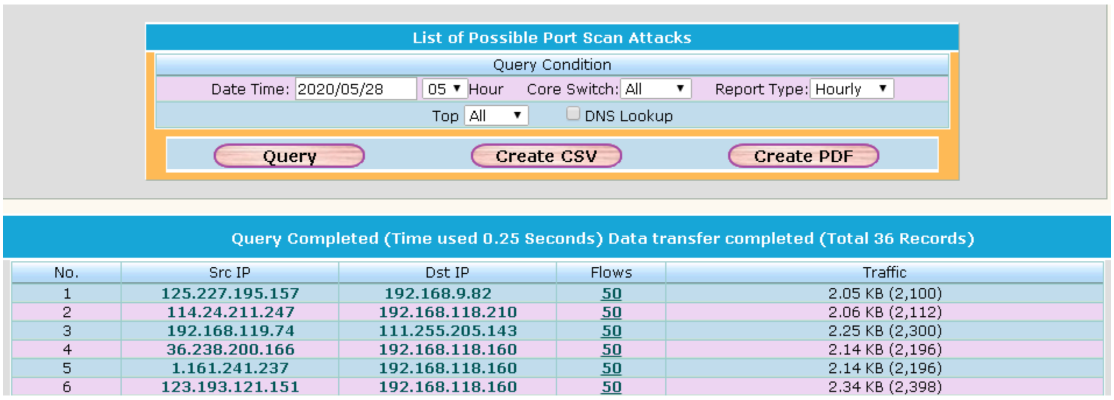
Query Completed (Time used 0.25 Seconds) Data transfer completed (Total 100 Records)

No.	Src IP	Dst IP	Flows	Traffic
1	211.201.69.50	192.168.102.17, ...	184	13.34 KB (13,664)
2	183.106.78.128	192.168.153.102, ...	155	12.11 KB (12,404)
3	62.103.236.182	192.168.107.180	136	25.26 KB (25,864)
4	217.23.8.88	140.128.105.175, ...	132	5.93 KB (6,072)
5	31.168.93.155	192.168.196.190	118	61.31 KB (62,779)
6	14.187.93.249	192.168.199.8	111	4.77 KB (4,882)
7	220.132.54.247	192.168.99.175	102	23.86 KB (24,430)
8	218.161.33.189	192.168.118.69	97	21.37 KB (21,884)
9	222.99.72.67	192.168.134.212, ...	86	3.91 KB (4,008)
10	112.209.140.131	192.168.107.180	85	16.09 KB (16,472)
11	112.134.164.153	192.168.130.23	84	15.20 KB (15,560)

Figure 56 – The report of telnet attack

Port Scan:

You can use the cross filter to find the port scanning attack records that you need in a report. You can also export the report to CSV / PDF file by clicking the **Create CSV/Create PDF** button.



List of Possible Port Scan Attacks

Query Condition

Date Time: 2020/05/28 | 05 Hour | Core Switch: All | Report Type: Hourly

Top All | □ DNS Lookup

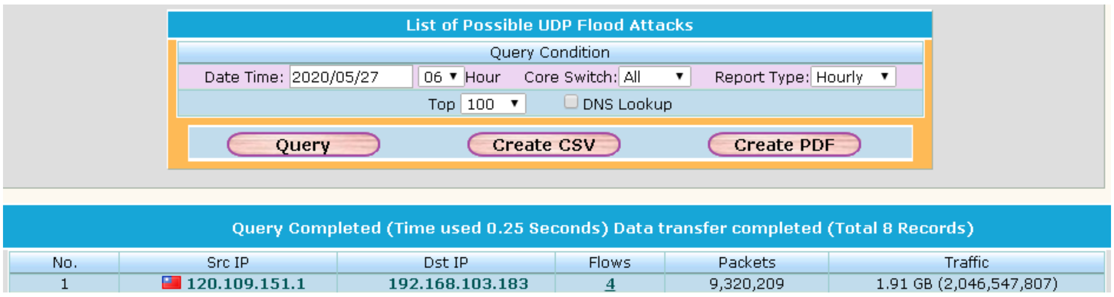
Query Completed (Time used 0.25 Seconds) Data transfer completed (Total 36 Records)

No.	Src IP	Dst IP	Flows	Traffic
1	125.227.195.157	192.168.9.82	50	2.05 KB (2,100)
2	114.24.211.247	192.168.118.210	50	2.06 KB (2,112)
3	192.168.119.74	111.255.205.143	50	2.25 KB (2,300)
4	36.238.200.166	192.168.118.160	50	2.14 KB (2,196)
5	1.161.241.237	192.168.118.160	50	2.14 KB (2,196)
6	123.193.121.151	192.168.118.160	50	2.34 KB (2,398)

Figure 57 – The report of port scanning

UDP Flood:

You can use the cross filter to find the UDP flooding attack records that you need in a report. You can also export the report to CSV / PDF file by clicking the **Create CSV/Create PDF** button.



List of Possible UDP Flood Attacks

Query Condition

Date Time: 2020/05/27 06 ▾ Hour Core Switch: All ▾ Report Type: Hourly ▾

Top 100 ▾ □ DNS Lookup

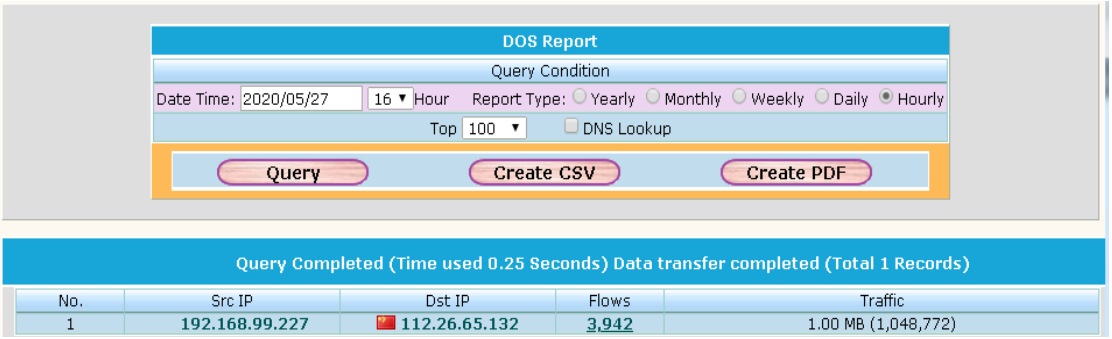
Query Completed (Time used 0.25 Seconds) Data transfer completed (Total 8 Records)

No.	Src IP	Dst IP	Flows	Packets	Traffic
1	120.109.151.1	192.168.103.183	4	9,320,209	1.91 GB (2,046,547,807)

Figure 58 – The report of UDP flooding attack

DOS Attack:

You can use the cross filter to find the DOS attack records that you need in a report. You can also export the report to CSV / PDF file by clicking the **Create CSV/Create PDF** button.



DOS Report

Query Condition

Date Time: 2020/05/27 16 ▾ Hour Report Type: ○ Yearly ○ Monthly ○ Weekly ○ Daily ● Hourly

Top 100 ▾ □ DNS Lookup

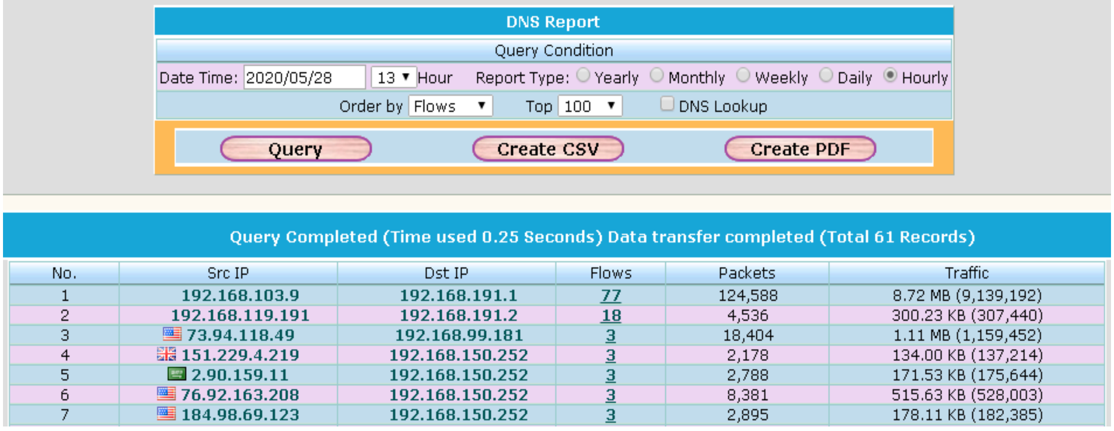
Query Completed (Time used 0.25 Seconds) Data transfer completed (Total 1 Records)

No.	Src IP	Dst IP	Flows	Traffic
1	192.168.99.227	112.26.65.132	3,942	1.00 MB (1,048,772)

Figure 59 – The report of DNS attack

DNS Attack:

You can use the cross filter to find the DNS attack records that you need in a report. You can also export the report to CSV / PDF file by clicking the **Create CSV/Create PDF** button.



DNS Report

Query Condition

Date Time: 2020/05/28 13 ▾ Hour Report Type: ○ Yearly ○ Monthly ○ Weekly ○ Daily ● Hourly

Order by Flows ▾ Top 100 ▾ □ DNS Lookup

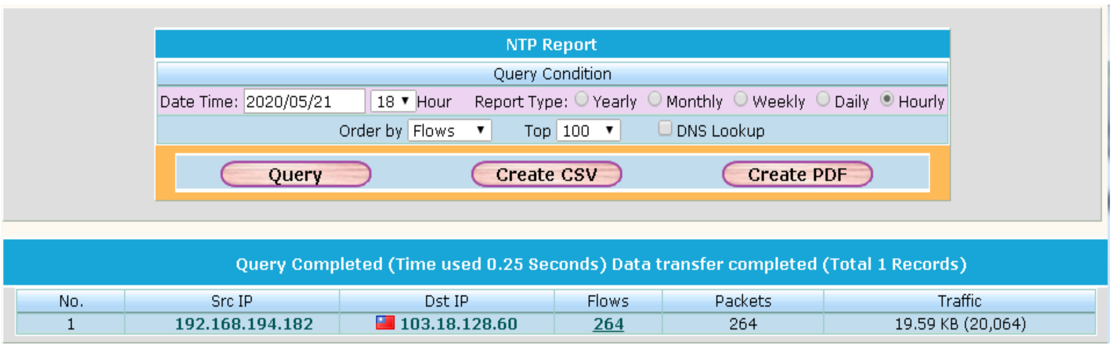
Query Completed (Time used 0.25 Seconds) Data transfer completed (Total 61 Records)

No.	Src IP	Dst IP	Flows	Packets	Traffic
1	192.168.103.9	192.168.191.1	77	124,588	8.72 MB (9,139,192)
2	192.168.119.191	192.168.191.2	18	4,536	300.23 KB (307,440)
3	73.94.118.49	192.168.99.181	3	18,404	1.11 MB (1,159,452)
4	151.229.4.219	192.168.150.252	3	2,178	134.00 KB (137,214)
5	2.90.159.11	192.168.150.252	3	2,788	171.53 KB (175,644)
6	76.92.163.208	192.168.150.252	3	8,381	515.63 KB (528,003)
7	184.98.69.123	192.168.150.252	3	2,895	178.11 KB (182,385)

Figure 60 – The report of DNS attack

NTP Attack:

You can use the cross filter to find the NTP attack records that you need in a report. You can also export the report to CSV / PDF file by clicking the **Create CSV**/**Create PDF** button.



NTP Report

Query Condition

Date Time: 2020/05/21 18 Hour Report Type: ○ Yearly ○ Monthly ○ Weekly ○ Daily ● Hourly

Order by Flows Top 100 □ DNS Lookup

Query Completed (Time used 0.25 Seconds) Data transfer completed (Total 1 Records)

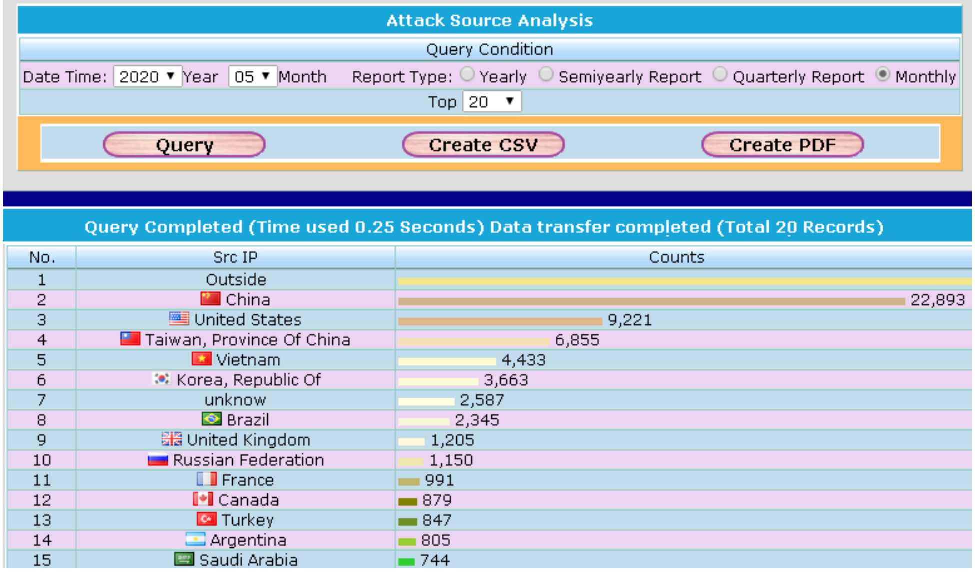
No.	Src IP	Dst IP	Flows	Packets	Traffic
1	192.168.194.182	103.18.128.60	264	264	19.59 KB (20,064)

Figure 61 – The report of NTP attack

Attack Source:

The system can provide a statistics for the attacking countries. It also counts the number of attacks that has been produced during the period. You can generate the monthly, quarterly, semiyearly and yearly report by selecting the 'Report Type'. This report can be exported to CSV / PDF file by clicking the **Create CSV**/**Create PDF** button. There are two special groups: Outside and unknown.

- **Outside:** This group includes the IP addresses which are not belong to your local area network (LAN).
- **unknown:** This group includes the IP addresses which cannot be identified.



Attack Source Analysis

Query Condition

Date Time: 2020 Year 05 Month Report Type: ○ Yearly ○ Semiyearly Report ○ Quarterly Report ● Monthly

Top 20

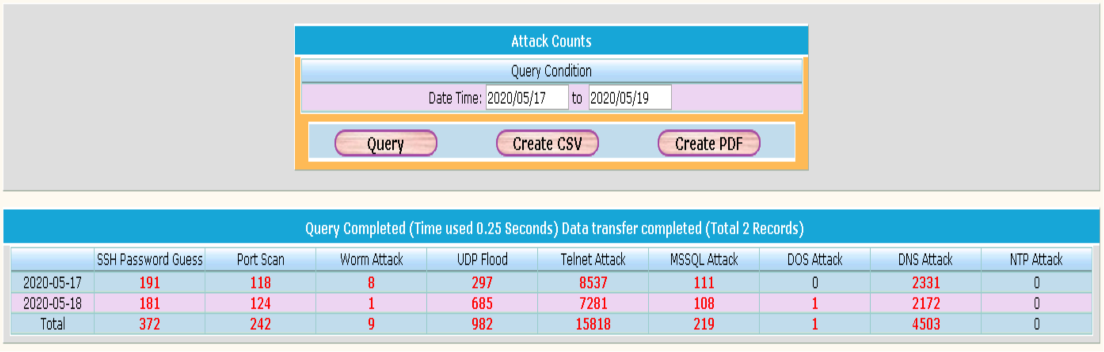
Query Completed (Time used 0.25 Seconds) Data transfer completed (Total 20 Records)

No.	Src IP	Counts
1	Outside	
2	China	22,893
3	United States	9,221
4	Taiwan, Province Of China	6,855
5	Vietnam	4,433
6	Korea, Republic Of	3,663
7	unknow	2,587
8	Brazil	2,345
9	United Kingdom	1,205
10	Russian Federation	1,150
11	France	991
12	Canada	879
13	Turkey	847
14	Argentina	805
15	Saudi Arabia	744

Figure 62 – The cybersecurity statistics

Attack Counts:

Flowwatch can provide the cyber security statistics for each kind of attack.



Attack Counts

Query Condition

Date Time: 2020/05/17 to 2020/05/19

Query Completed (Time used 0.25 Seconds) Data transfer completed (Total 2 Records)

	SSH Password Guess	Port Scan	Worm Attack	UDP Flood	Telnet Attack	MSSQL Attack	DOS Attack	DNS Attack	NTP Attack
2020-05-17	191	118	8	297	8537	111	0	2331	0
2020-05-18	181	124	1	685	7281	108	1	2172	0
Total	372	242	9	982	15818	219	1	4503	0

Figure 63 – The cybersecurity statistics

Public Report

Sometimes you may want to share reports with someone who doesn't have an account. For the Top N report, the administrator can hide the information of the specific IP addresses. For more on this, refer to this section.

Traffic Graphic:

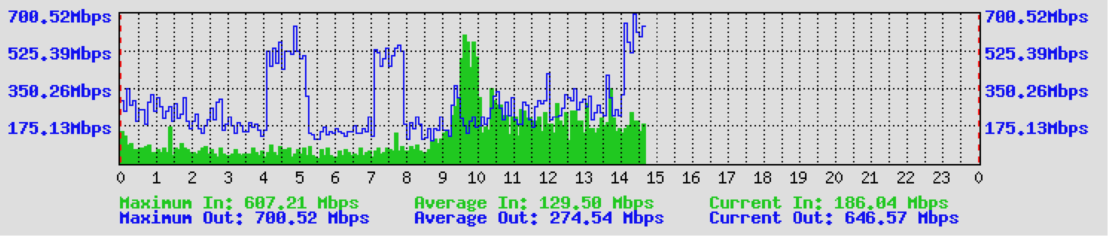
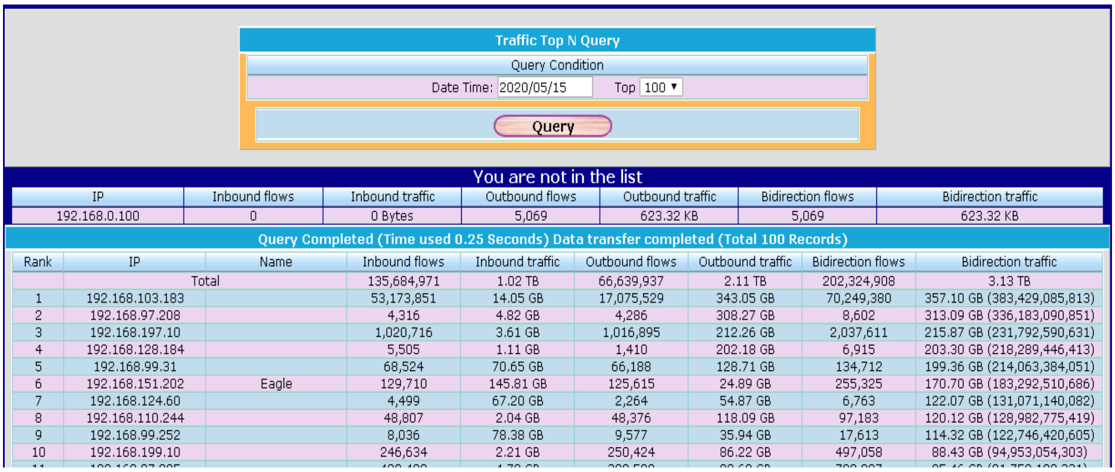


Figure 64 – The public Network Traffic

Top N:



Date Time: 2020/05/15 Top 100

You are not in the list

IP	Inbound flows	Inbound traffic	Outbound flows	Outbound traffic	Bidirection flows	Bidirection traffic
192.168.0.100	0	0 Bytes	5,069	623.32 KB	5,069	623.32 KB

Query Completed (Time used 0.25 Seconds) Data transfer completed (Total 100 Records)

Rank	IP	Name	Inbound flows	Inbound traffic	Outbound flows	Outbound traffic	Bidirection flows	Bidirection traffic
	Total		135,684,971	1.02 TB	66,639,937	2.11 TB	202,324,908	3.13 TB
1	192.168.103.183		53,173,851	14.05 GB	17,075,529	343.05 GB	70,249,380	357.10 GB (383,429,085,813)
2	192.168.97.208		4,316	4.82 GB	4,286	308.27 GB	8,602	313.09 GB (336,183,090,851)
3	192.168.197.10		1,020,716	3.61 GB	1,016,895	212.26 GB	2,037,611	215.87 GB (231,792,590,631)
4	192.168.128.184		5,505	1.11 GB	1,410	202.18 GB	6,915	203.30 GB (218,289,446,413)
5	192.168.99.31		68,524	70.65 GB	66,188	128.71 GB	134,712	199.36 GB (214,063,384,051)
6	192.168.151.202	Eagle	129,710	145.81 GB	125,615	24.89 GB	255,325	170.70 GB (183,292,510,686)
7	192.168.124.60		4,499	67.20 GB	2,264	54.87 GB	6,763	122.07 GB (131,071,140,082)
8	192.168.110.244		48,807	2.04 GB	48,376	118.09 GB	97,183	120.12 GB (128,982,775,419)
9	192.168.99.252		8,036	78.38 GB	9,577	35.94 GB	17,613	114.32 GB (122,746,420,605)
10	192.168.199.10		246,634	2.21 GB	250,424	86.22 GB	497,058	88.43 GB (94,953,054,303)

Figure 65 – Top N report

Note: The trial version can only display the first 30 records.